Project acronym: CRISP
Project title: Evaluation and Certification Schemes for Security Products
Grant number: 607941
Programme: Seventh Framework Programme for Security
Objective: Topic SEC-2013.5.4-1 Evaluation and certification schemes for security products
Contract type: Capability project
Start date of project: 01 April 2014
Duration: 36 months
Website: www.crispproject.eu

Deliverable D 2.2:
Consolidated report on security standards, certification and accreditation – best practice and lessons learnt

Authors: Dr. Simone Wurster, Dr. Tim Pohlmann, Nathalie Hirschmann and Dr. Patrick Murphy (TU Berlin), Jolien van Zetten, Ying Ying Lau and Dr. Tatsiana Haponava (NEN), Dr. Thordis Sveinsdottir, Rachel Finn, Rowena Rodrigues, Kush Wadhwa (Trilateral Research), Dr. Reinhard Kreissl, Dr. Florian Fritz, Roger von Laufenberg (VICESSE), Prof. Cristina Pauner, Artemi Rallo, Rosario García Mahamut and Jorge Viguri (UJI), Irene Kamara, Prof. Paul de Hert (VUB), Eva Kalan, Jelena Burnik and Igor Kolar (IP-RS)

Dissemination level: Public
Deliverable type: Final
Version: 1.1
31 January 2017
CRISP has received funding from the European Union’s Seventh Framework Program for research, technological development and demonstration under grant agreement no 607941. Re-use of information contained in this document for commercial and/or non-commercial purposes is authorised and free of charge, on the conditions of acknowledgement by the re-user of the source of the document, not distortion of the original meaning or message of the document and the non-liability of the CRISP consortium and/or partners for any consequence stemming from the re-use. The CRISP consortium does not accept responsibility for the consequences, errors or omissions herein enclosed. This document is subject to updates, revisions and extensions by the CRISP consortium. Questions and comments should be addressed to: crisp@nen.nl.
<table>
<thead>
<tr>
<th>Version number</th>
<th>Date</th>
<th>Sections</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>30th June 2015</td>
<td>all</td>
<td>Dr. Simone Wurster, Dr. Tim Pohlmann, Nathalie Hirschmann and Dr. Patrick Murphy (TU Berlin), Jolien van Zetten, Ying Ying Lau and Dr. Tatsiana Haponava (NEN), Dr. Thordis Sveinsdottir, Rachel Finn, Rowena Rodrigues, Kush Wadhwa (Trilateral Research), Dr. Reinhard Kreissl, Dr. Florian Fritz, Roger von Laufenberg (VICESSE), Prof. Cristina Pauner, Artemi Rallo, Rosario García Mahmut and Jorge Viguri (UJI), Irene Kamara, Prof. Paul de Hert (VUB), Eva Kalan, Jelena Burnik and Igor Kolar (IP-RS)</td>
</tr>
</tbody>
</table>
| Version 1.1    | 19th January 2017 | • chapter 1  
• last subchapters of the country studies  
• chapter 9.3 added  
• previous chapter 9.3, which is 9.4 now, updated  
• minor additional changes | Dr. Simone Wurster (TU Berlin) |
TABLE OF CONTENTS

List of figures ................................................................................................................................. 12
List of selected abbreviations ........................................................................................................ 17

1. Introduction ............................................................................................................................... 20
2. Conformity assessment: an important tool for market coordination ........................................ 24
3. European country studies .......................................................................................................... 29
3.1. Austria ...................................................................................................................................... 29
3.1.1. Introduction .......................................................................................................................... 29
3.1.2. Short description of Austria’s security industry ................................................................. 29
3.1.3. The security standardisation framework ............................................................................. 33
3.1.4. The security conformity assessment framework ............................................................... 36
3.1.5. Selected security certification bodies and their work ........................................................ 39
3.1.6. Summary and conclusion ................................................................................................. 47
3.1.7. References ......................................................................................................................... 49

3.2. Belgium .................................................................................................................................. 51
3.2.1. Introduction ........................................................................................................................ 51
3.2.2. Short description of Belgium’s security industry ............................................................... 51
3.2.3. The security standardisation framework ......................................................................... 52
3.2.4. The security conformity assessment framework ............................................................. 56
3.2.5. Selected security certification bodies and their work ....................................................... 58
3.2.5.1. Certification schemes ...................................................................................................... 58
3.2.5.2. Selected certification bodies ............................................................................................ 59
3.2.6. Summary and conclusion ................................................................................................. 63
3.2.7. References ......................................................................................................................... 64

3.3. France ..................................................................................................................................... 66
3.3.1. Introduction ........................................................................................................................ 66
3.3.2. Short description of the country’s security industry .......................................................... 66
3.3.2.1. The administrative structure of France ........................................................................ 66
3.3.2.2. The French security market ........................................................................................... 67
3.3.3. The security standardisation framework ......................................................................... 69
3.3.3.1. The French security system .......................................................................................... 69
3.3.3.2. Security standardisation at AFNOR ............................................................................. 70
3.3.3.3. The French GIS - Security and Citizen Protection Group ...................................... 74
3.3.3.4. Specific standardisation issues ..................................................................................... 77
3.3.4. The security conformity assessment framework ............................................................. 78
3.3.5. Selected security certification bodies and their work ....................................................... 81
3.3.6. Summary and conclusion ................................................................................................. 86

Page 4 of 542
3.7.3.2. The Aviation Safety and security agency AESA and accredited organisations .............................................................. 156
3.7.4. The security conformity assessment framework .......................................................... 160
3.7.5. Selected security certification bodies and their work ......................................................... 165
3.7.5.1. Selected private certification bodies ................................................................................. 165
3.7.5.2. Certification at the National Cryptologic Centre (CCN) ....................................................... 171
3.7.6. Examples for the use of security standards for certification in Spain ................................. 172
3.7.7. Certification of drones ...................................................................................................... 173
3.7.8. Summary and conclusion ............................................................................................... 181
3.7.9. References ...................................................................................................................... 182
3.7.10. Annex ............................................................................................................................ 184
3.8. Sweden .................................................................................................................................. 186
3.8.1. Short description of Sweden’s security industry ................................................................. 186
3.8.2. The security standardisation framework .......................................................................... 187
3.8.3. The security conformity assessment framework ............................................................... 189
3.8.4. Selected security certification bodies and their work ......................................................... 192
3.8.4.1. Private certification bodies ............................................................................................. 192
3.8.4.2. Public sector .................................................................................................................. 199
3.8.5. Summary and conclusion ............................................................................................... 203
3.8.6. References ...................................................................................................................... 203
3.9. United Kingdom .................................................................................................................. 205
3.9.1. Introduction ...................................................................................................................... 205
3.9.2. Short description of the UK security industry ................................................................. 205
3.9.2.1. Selected Policy, Regulation and legislation ................................................................. 206
3.9.2.2. The British Security Industry Association (BSIA) ......................................................... 209
3.9.3. The security standardisation framework .......................................................................... 213
3.9.3.1. British Standards Agency (BSI) ..................................................................................... 214
3.9.3.2. The UK Accreditation Service (UKAS) ....................................................................... 216
3.9.3.3. UK ISO TC participation .............................................................................................. 216
3.9.4. Selected EN and ISO Standards and their application in the UK ........................................ 217
3.9.5. The security conformity assessment framework ............................................................... 217
3.9.6. Selected security certification bodies and their work ......................................................... 219
3.9.7. Governmental organisations responsible for conformity assessment in the security field .......................................................................................................................... 228
3.9.8. Summary and conclusion ............................................................................................... 231
3.9.9. References ...................................................................................................................... 232
3.10. The Netherlands ................................................................................................................ 234
3.10.1. Short description of the security industry in the Netherlands ........................................... 234
D2.2: Consolidated report on security standards and certification

3.10.2. Security standardisation framework ................................................................. 234
3.10.3. Conformity assessment framework ................................................................. 235
3.10.3.1. Certification bodies – overview ................................................................. 235
3.10.3.2. Certification bodies – in depth ................................................................. 236
3.10.4. Summary and conclusions ............................................................................. 238
3.10.5. References ..................................................................................................... 238
3.11. Final remarks on chapter 3 ............................................................................. 239
4. International country studies ............................................................................. 242
4.1. United States ...................................................................................................... 242
4.1.1. Introduction .................................................................................................... 242
4.1.2. Short description of the country’s security industry ........................................ 243
4.1.3. The security standardisation framework ....................................................... 245
4.1.3.1. The security standardisation system in general ........................................ 245
4.1.3.2. Relevant legislation ................................................................................... 247
4.1.3.3. Work of selected standard development organisations ............................ 250
4.1.3.4. National Strategy for CBRNE Standards ................................................. 259
4.1.4. The security conformity assessment framework ............................................. 261
4.1.5. Selected security certification bodies and their work ...................................... 263
4.1.5.1. Public sector ............................................................................................. 263
4.1.5.2. Private certification bodies ....................................................................... 272
4.1.5.3. Industry organisations ............................................................................ 281
4.1.6. Summary and conclusion ............................................................................. 285
4.1.7. References ..................................................................................................... 286
4.2. Canada ................................................................................................................ 291
4.2.1. Introduction .................................................................................................... 291
4.2.2. Short description of the country’s security industry ........................................ 291
4.2.3. The standardisation and accreditation process .............................................. 292
4.2.4. The security standardisation framework ....................................................... 293
4.2.5. The security conformity assessment framework ............................................. 297
4.2.6. Selected security certification bodies and their work ...................................... 299
4.2.7. Summary and conclusion ............................................................................. 317
4.2.8. References ..................................................................................................... 318
4.3. Brazil .................................................................................................................. 320
4.3.1. Introduction .................................................................................................... 320
4.3.2. Short description of the country’s security industry ........................................ 320
4.3.3. The security standardisation framework ....................................................... 322
4.3.3.1. Introduction ................................................................. 322
4.3.3.2. Specific security standards ........................................... 323
4.3.3.3. International activities in the security field ..................... 325
4.3.4. The security conformity assessment framework .................. 326
4.3.5. Selected security certification bodies and their work .......... 330
4.3.5.1. Public sector ............................................................ 330
4.3.5.2. Private conformity assessment bodies .......................... 332
4.3.6. Summary and conclusion ............................................... 333
4.3.7. References .................................................................... 333
4.4. India .................................................................................. 335
4.4.1. Introduction .................................................................... 335
4.4.2. Short description of India’s security industry .................... 335
4.4.3. The security standardisation framework ............................ 337
4.4.4. Selected security certification bodies and their work .......... 349
4.4.5. Summary and conclusion ............................................... 359
4.4.6. References ..................................................................... 359
4.5. Israel ................................................................................... 362
4.5.1. Introduction .................................................................... 362
4.5.2. Short description of the Israel security industry ............... 362
4.5.2.1. Key figures .................................................................. 362
4.5.2.2. Cyber security strategy of Israel .................................. 365
4.5.3. The security standardisation framework and relevant regulations ........................................ 366
4.5.3.1. The Standards Institution of Israel ............................... 367
4.5.3.2. Israel’s ISO participation ............................................ 367
4.5.4. The security conformity assessment framework ................ 368
4.5.4.1. Conformity assessment in Israel in general ................... 368
4.5.4.2. Conformity assessment framework in the security field 370
4.5.5. Summary and conclusions ............................................... 370
4.5.6. References ..................................................................... 371
4.6. Japan .................................................................................... 374
4.6.1. Introduction .................................................................... 374
4.6.2. Japan’s security industry ............................................... 374
4.6.3. Security standardisation framework ................................ 376
4.6.4. Security conformity assessment framework .................... 380
4.6.5. Selected security certification bodies and their work .......... 382
4.6.6. Recent developments and current security market trends .... 383
4.6.7. Identification of good practices approaches ...................... 383
D2.2: Consolidated report on security standards and certification

4.6.8. Summary and conclusion .......................................................... 384
4.6.9. References ............................................................................ 384
5. International standardisation activities ............................................. 387
5.1. Introduction ................................................................................ 387
5.2. Overview of Technical Committees ............................................. 387
5.3. Work of specific Technical Committees ....................................... 388
5.4. Standards related to specific CRISP dimensions ......................... 402
5.5. Summary and conclusion ............................................................ 404
5.6. References ................................................................................ 405
6. Pan-European certification schemes .............................................. 406
6.1. Introduction ................................................................................ 406
6.2. Detection Systems, Security Scanners and Screening Equipment .... 407
6.3. Security Alarm Systems ............................................................... 410
6.4. Remotely Piloted Aircraft Systems ............................................. 412
6.5. Privacy Seals ............................................................................ 416
6.6. Authorised Economic Operator .................................................. 417
6.7. CE Marking ................................................................................ 419
6.8. The ‘EU Security Label’ .............................................................. 420
6.9. References ................................................................................ 422
7. International certification schemes ................................................. 427
7.1. Introduction ................................................................................ 427
7.2. Security of the citizens – Crime Prevention .................................. 427
7.2.1. Open Network Video Interface Forum (ONVIF) ......................... 427
7.2.2. International Code of Conduct for Private Security Service Providers .... 430
7.3. Security of the citizens – Privacy ................................................ 432
7.4. Security of the Citizens / Security of the Infrastructure – Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) .... 435
7.4.1. CREATIF Project .................................................................. 436
7.4.2. IAEA Nuclear Security Series ................................................ 436
7.5. Security of infrastructure – Supply Chain Security ....................... 439
7.6. Security and Crisis Management ............................................... 444
7.7. Border Security in general .......................................................... 445
7.7.1. Passenger Name Record data ................................................. 446
7.7.2. Customs-Trade Partnership Against Terrorism (C-TPAT) ........... 447
7.8.1. International Ship and Port Facility Security Code ..................... 450
D2.2: Consolidated report on security standards and certification

7.8.3. Container Security Initiative (CSI) ................................................................. 453
7.8.4. Information security - Common Criteria ....................................................... 457
7.8.4.1. Introduction ................................................................................................. 457
7.8.4.2. The Common Criteria framework .............................................................. 457
7.8.4.3. Common Criteria Certification Schemes .................................................... 462
7.8.4.4. Summary ..................................................................................................... 464
7.9. Conclusion .......................................................................................................... 466
7.10. References .......................................................................................................... 467
8. Accreditation of certification bodies in the security field ........................................ 472
8.1. Current state of play in accreditation in Europe .................................................. 472
8.1.1. Standards on accreditation and their implementation in Europe .................... 472
8.1.2. EU Regulation 765/2008 .............................................................................. 478
8.1.3. The European Accreditation framework – History and future plans ............... 483
8.1.4. Principles of the European Cooperation for Accreditation ............................ 485
8.1.4.1. Basic requirements according to ISO and the IEC ................................. 485
8.1.4.2. Specific EA requirement sets on conformity assessment schemes ............ 485
8.1.4.3. Topics for the validation of certification schemes ....................................... 486
8.1.4.4. Acceptance of assessment schemes by European Accreditation Bodies .... 488
8.1.4.5. Duties of scheme owners ........................................................................ 488
8.1.4.6. Multinational CASs ................................................................................ 489
8.1.5. Specifics in the security field ......................................................................... 489
8.2. Implementation of Regulation 765/2008 in selected European countries ............ 490
8.2.1. France ........................................................................................................ 490
8.2.2. Germany .................................................................................................... 495
8.2.3. Italy ............................................................................................................. 500
8.2.4. Slovenia ..................................................................................................... 501
8.2.5. Spain .......................................................................................................... 505
8.2.6. Poland ....................................................................................................... 509
8.2.7. Romania ..................................................................................................... 511
8.2.8. The United Kingdom ................................................................................ 512
8.2.9. Other countries .......................................................................................... 515
8.3. International frameworks and acceptance of European Conformity Assessment .... 518
8.3.1. Introduction to international frameworks and mutual recognition .................. 518
8.3.2. The International Laboratory Accreditation Cooperation (ILAC) ................. 520
8.3.3. The Inter-American Accreditation Cooperation (IAAC) ............................... 524
LIST OF FIGURES

Figure 1: Benefits of conformity assessment to main groups of stakeholders ........................................... 24
Figure 2: Functional approach to conformity assessment ........................................................................... 26
Figure 3: Number of security and investigation companies in Austria per state ......................................... 30
Figure 4: Monitoring and alarm receiving centres in Austria ..................................................................... 30
Figure 5: Austria’s participation in relevant security related ISO TCs ........................................................ 35
Figure 6: Selected standards as a basis for certification in Austria ............................................................. 38
Figure 7: Overview of important (security) certification bodies in Austria ................................................. 39
Figure 8: Overview of Belgian legislation for standardisation activities .................................................... 52
Figure 9: Representation of the decentralized standardisation system in Belgium ..................................... 53
Figure 10: European and international TCs on security and relevant sector operators in Belgium .......... 53
Figure 11: NBN homegrown security standards ......................................................................................... 54
Figure 12: Overview of Belgian legislation for accreditation ....................................................................... 57
Figure 13: Belgian accreditation body and characteristics .......................................................................... 57
Figure 14: Belgian accreditation system ..................................................................................................... 58
Figure 15: Overview of important (security) certification bodies in Belgium ............................................. 58
Figure 16: Example of the INCERT certification framework for remote surveillance centers .................... 59
Figure 17: Documents for ANPI certification activities ............................................................................... 61
Figure 18: ANPI quality seals ...................................................................................................................... 61
Figure 19: Security standards topics in France ............................................................................................ 71
Figure 20: Standards issued by ISO/TC 223 with French contribution ....................................................... 72
Figure 21: The key groups in security standardisation with French involvement ...................................... 75
Figure 22: The French position for civil security ......................................................................................... 76
Figure 23: Accredited certifications from COFRAC in the security field .................................................. 81
Figure 24: Security certification schemes in France .................................................................................... 82
Figure 25: Estimation of the turnover of the German security industry based on different studies ........... 90
Figure 26: Security turnover in Germany by technology segments ............................................................. 91
Figure 27: DIN’s and DKE’s involvement in European and international standards development ......................... 92
Figure 28: Germany’s participation in selected ISO TCs .......................................................................... 96
Figure 29: Overview of selected security-related certification bodies in Germany .................................... 99
Figure 30: German CABs related to selected security standards ................................................................. 100
Figure 31: Aviation security authorities in Germany .................................................................................... 101
Figure 32: Test centers for IT security and cryptography in Germany ....................................................... 104
Figure 33: Suggestion for the European certification landscape by German stakeholders ................................................................. 105
Figure 34: Data protection seals available at the datenschutz cert GmbH ................................................................. 116
Figure 35: Key figures of Poland’s security industry compared with other EU countries ................................................................. 126
Figure 36: PKN’s TCs in the security field .................................................................................................................. 128
Figure 37: Poland’s involvement in selected ISO/IEC TCs .......................................................................................... 129
Figure 38: Overview of security certification services in Poland .............................................................................. 130
Figure 39: CNBOP’s certification mark ..................................................................................................................... 131
Figure 40: Elements of CNBOP’s certification of services ......................................................................................... 132
Figure 41: SIST’s membership in security-related ISO TCs ....................................................................................... 138
Figure 42: List of some exemplary EN standards that are mandatory for private Slovenian companies to be compliant with .................................................................................................................. 140
Figure 43: Spain’s participation in selected ISO TCs ................................................................................................. 155
Figure 44: Key organisations in Spain’s security-related conformity assessment framework ............................................. 161
Figure 45: Accredited Spanish certification bodies for selected security standards .......................................................... 163
Figure 46: Overview of selected CABs in the security field in Spain ........................................................................... 164
Figure 47: Principles for the certification of drones in Spain .......................................................................................... 176
Figure 48: Sweden’s involvement in selected ISO/IEC TCs ....................................................................................... 188
Figure 49: Swedish landscape of security certification and inspection services ................................................................. 189
Figure 50: Overview of Swedish CABs in the security field ........................................................................................... 190
Figure 51: Selected standards as a basis for certification in Sweden .............................................................................. 191
Figure 52: Overview of security standards used by DNV Sweden ................................................................................ 193
Figure 53: SBSC’s certification mark ....................................................................................................................... 194
Figure 54: Categorisation of UAV activities in Sweden ............................................................................................... 201
Figure 55: UK security sub sectors ............................................................................................................................ 206
Figure 56: Key standards for the British security industry .......................................................................................... 213
Figure 57: The UK quality infrastructure .................................................................................................................. 213
Figure 58: Origin of currently used security standards in the UK .................................................................................. 215
Figure 59: British participation in selected ISO TCs .................................................................................................. 217
Figure 60: British certification bodies in selected fields ............................................................................................. 217
Figure 61: Overview of British certification bodies and their services in the security field ...................................................... 218
Figure 62: BSI secure digital transactions KITEMARK™ .............................................................................................. 220
Figure 63: Relevant standards for BSI’s certification services in the security field ......................................................... 220
Figure 64: LPCB certification mark ............................................................................................................................ 221
Figure 65: BRE/LPCB layering of standards for a holistic approach to security .............................................................. 222
Figure 66: NSI Gold and Silver Certification Seals ........................................................................................................ 223
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 67</td>
<td>NSI solutions in the field of electronic security</td>
<td>224</td>
</tr>
<tr>
<td>Figure 68</td>
<td>NSI solutions in the fields of guarding and cash services</td>
<td>226</td>
</tr>
<tr>
<td>Figure 69</td>
<td>Areas of the Approved Contractor Scheme</td>
<td>228</td>
</tr>
<tr>
<td>Figure 70</td>
<td>The CESG Certification Mark</td>
<td>229</td>
</tr>
<tr>
<td>Figure 71</td>
<td>Standards which a relevant for receiving business licence for security services in the UK</td>
<td>230</td>
</tr>
<tr>
<td>Figure 72</td>
<td>Accredited certification bodies in the security field in The Netherlands</td>
<td>237</td>
</tr>
<tr>
<td>Figure 73</td>
<td>U.S. HLS &amp; public safety market (2007-2020)</td>
<td>243</td>
</tr>
<tr>
<td>Figure 74</td>
<td>U.S. involvement in selected security-related ISO TCs</td>
<td>247</td>
</tr>
<tr>
<td>Figure 75</td>
<td>NIJ standards in the security field</td>
<td>254</td>
</tr>
<tr>
<td>Figure 76</td>
<td>Important private security certification bodies in the U.S.</td>
<td>262</td>
</tr>
<tr>
<td>Figure 77</td>
<td>Accreditation bodies in the U.S.</td>
<td>263</td>
</tr>
<tr>
<td>Figure 78</td>
<td>Elements of the SAFETY Act</td>
<td>265</td>
</tr>
<tr>
<td>Figure 79</td>
<td>SAFETY Act seals</td>
<td>265</td>
</tr>
<tr>
<td>Figure 80</td>
<td>Elements of the SAFETY Act</td>
<td>268</td>
</tr>
<tr>
<td>Figure 81</td>
<td>Timeline of SAFETY Act applications</td>
<td>268</td>
</tr>
<tr>
<td>Figure 82</td>
<td>Intertek marks</td>
<td>279</td>
</tr>
<tr>
<td>Figure 83</td>
<td>Standards used for Intertek’s certification of central stations</td>
<td>281</td>
</tr>
<tr>
<td>Figure 84</td>
<td>CSPM® certification process</td>
<td>282</td>
</tr>
<tr>
<td>Figure 85</td>
<td>Canada’s involvement in selected security-related ISO TCs</td>
<td>297</td>
</tr>
<tr>
<td>Figure 86</td>
<td>Brazil’s involvement in selected security-related ISO TCs</td>
<td>326</td>
</tr>
<tr>
<td>Figure 87</td>
<td>The Brazilian System of Conformity Assessment</td>
<td>327</td>
</tr>
<tr>
<td>Figure 88</td>
<td>Organisations and duties in the Brazilian conformity assessment system</td>
<td>328</td>
</tr>
<tr>
<td>Figure 89</td>
<td>India ISO TC participation for selected standards development</td>
<td>339</td>
</tr>
<tr>
<td>Figure 90</td>
<td>Development of Indian standards</td>
<td>342</td>
</tr>
<tr>
<td>Figure 91</td>
<td>BIS standards activity 2012-2014</td>
<td>343</td>
</tr>
<tr>
<td>Figure 92</td>
<td>Indian security equipment standards</td>
<td>344</td>
</tr>
<tr>
<td>Figure 93</td>
<td>Indian security equipment standards under print</td>
<td>344</td>
</tr>
<tr>
<td>Figure 94</td>
<td>System security and biometric standards in India</td>
<td>345</td>
</tr>
<tr>
<td>Figure 95</td>
<td>Draft system security and biometric standards in India</td>
<td>346</td>
</tr>
<tr>
<td>Figure 96</td>
<td>Alarms and electronic security systems standards in India</td>
<td>347</td>
</tr>
<tr>
<td>Figure 97</td>
<td>Conformity assessment, testing &amp; certification in India</td>
<td>350</td>
</tr>
<tr>
<td>Figure 98</td>
<td>ISI Certification Mark</td>
<td>350</td>
</tr>
<tr>
<td>Figure 99</td>
<td>Foreign manufacturers licenses granted in India</td>
<td>351</td>
</tr>
<tr>
<td>Figure 100</td>
<td>Process for CC certification in India</td>
<td>358</td>
</tr>
<tr>
<td>Figure 101</td>
<td>Israel’s security sector division in percent</td>
<td>363</td>
</tr>
<tr>
<td>Figure 102</td>
<td>Initiating and approving standards in Israel</td>
<td>367</td>
</tr>
<tr>
<td>Figure 103</td>
<td>Israel’s involvement in selected security-related ISO TCs</td>
<td>368</td>
</tr>
</tbody>
</table>
Figure 104: Accreditation process by ISRAC

Figure 105: Common standards of the IQC

Figure 106: Mutual Recognition Agreements between SII and U.S. organisations

Figure 107: JIS logo

Figure 108: Standardisation activities at JIS across industries

Figure 109: JIS development process

Figure 110: Japan’s involvement in selected security-related ISO TCs

Figure 111: Overview of the activities of ISO TC 68

Figure 112: Overview of the activities of ISO TC 85

Figure 113: Overview of the activities of ISO TC 92

Figure 114: Overview of the activities of ISO TC 94

Figure 115: Overview of the activities of ISO TC 207

Figure 116: Overview of the activities of ISO TC 224

Figure 117: Overview of the activities of ISO TC 262

Figure 118: Overview of the activities of ISO TC 292

Figure 119: Overview of the activities of ISO/IEC JTC 1/SC 17

Figure 120: Overview of the activities of ISO/IEC JTC 1/SC 27

Figure 121: Overview of the activities of ISO/IEC JTC 1/SC 31

Figure 122: Selected international and European standards in the area of privacy and data protection

Figure 123: ECAC’s current accomplishments

Figure 124: Institutions involved in the harmonization of RPAS

Figure 125: Categorisation of drone operations

Figure 126: Roadmap for the certification of RPAS in Europe

Figure 127: ONVIF profiles

Figure 128: ICoC principles

Figure 129: WCO customs-to-customs specifications

Figure 130: AEO specifications

Figure 131: CSI screening process of containers

Figure 132: The signatory countries of the Common Criteria Recognition Arrangement

Figure 133: Common Criteria logo

Figure 134: Common Criteria evaluation assurance levels and content

Figure 135: Overview of standards pertaining to conformity assessment and their scopes

Figure 136: Overview of techniques used in major types of product certification schemes

Figure 137: Use of important accreditation standards in the EU
Figure 138: Accreditation and certification in France .......................................................... 491
Figure 139: Divisions of Germany’s DAkkS ................................................................. 496
Figure 140: The accreditation process at DAkkS .......................................................... 496
Figure 141: Example of the DAkkS accreditation symbol with unique registration number .................................................................................................................... 497
Figure 142: Number of accreditations in previous years in Slovenia ......................... 503
Figure 143: Mutual recognition of laboratory and inspection team accreditation under ILAC ......................................................................................................................................... 519
Figure 144: EU ILAC members and the standards they currently accredit to .............. 523
LIST OF SELECTED ABBREVIATIONS

AEO  Authorised Economic Operator
AFNOR Association Française de Normalisation
ANSI American National Standards Institute
APLAC Asia Pacific Laboratory Accreditation Cooperation
ASI Austrian Standards Institute
BSI (DEU) Bundesamt für Sicherheit in der Informationstechnik
BSI (GB) British Standards Institution
CA Conformity Assessment
CAB Conformity Assessment Body
CAS Conformity Assessment System
CB Certification body
CBRN Chemical, Biological, Radiological and Nuclear
CBRNE Chemical, Biological, Radiological, Nuclear and Explosive
CC Common Criteria
CCRA Common Criteria Recognition Agreement
CCTV Closed-circuit television
CEN Comité Européen de Normalisation
CENELEC Comité Européen de Normalisation Electrotechnique
CEOC International Confederation of Inspection and Certification Organisations
CLC CENELEC
CoESS Confederation of European security services
COM Communication
CPR Construction Products Regulation
CREATIF Network of Testing Facilities for CBRNE detection equipment
CRISP Evaluation and Certification Schemes for Security Products
CWA CEN Workshop Agreement
DAkkS Deutsche Akkreditierungsstelle GmbH
DHS Department of Homeland Security
DIN Deutsches Institut für Normung
DOJ Department of Justice
EA European co-operation for Accreditation
ECAC European Civil Aviation Conference
ECB European Certification Body
EEA European Economic Area
EFAC European Federation of Associations of Certification bodies
EFSG European Fire and Security Group
EFTA European Free Trade Association
EN European Norm
ENISA European Union Agency for Network and Information Security
EOTC European Organisation for Testing and Certification
ESOs European Standardisation Organisations
ESRIA European Security Research and Innovation Agenda
ESRIF European Security Research and Innovation Forum
ETSI European Telecommunications Standards Institute
FIPS  Federal Information Processing Standards
hAB  Homa Accreditation Body
IAAC  Inter America Accreditation Cooperation
IAF  International Accreditation Forum
ICT  Information and communications technology
IEC  International Electrotechnical Commission
IIOC  Independent International Organisation for Certification
ILAC  International Laboratory Accreditation Cooperation
ISO  International Organization for Standardisation
ISMS  Information Security Management System
IT  Information Technology
ITSEC  Information Technology Security Evaluation Criteria
ITU  International Telecommunication Union
IWA  Internationale Workshop Agreement
JTC  Joint Technical Committee
LPCB  Loss Prevention Certification Board
LRQA  Lloyd’s Register Quality Assurance
MLA  Multilateral Agreement/Multilateral Recognition Arrangement
MRA  Mutual Recognition Agreement
NAB  National accreditation body
NACE  Statistical Classification of Economic Activities in the European Community
NBN  Belgian Bureau for Standardisation
NEN  Nederlandse Norm (National Standardisation Body of the Netherlands)
NLF  New Legislative Framework
NSB  National Standardisation Body
NTTAA  National Technology Transfer and Advancement Act
PAC  Pacific Accreditation Cooperation
PCA  Policy Certification Authority
PKN  Polish Committee for Standardization
prEN  project of European Norm
PSS  products, systems and services
RPA  Remotely Piloted (civil) Aircraft
RPAS  Remotely Piloted (civil) Aircraft System
SA  Slovenian Accreditation
SADCA  Southern African Development Community Accreditation
SBSC  Svensk Brand- och Säkerhetscertifiering AB
SC  Sub Committee
SIS  Swedish Standards Institute
SIST  Slovenian Institute for Standardization
SMEs  Small- and Medium-sized Enterprises
SO  Scheme Owner
SOG-IS  Senior Officials Group Information System Security
TC  Technical Committee
TR  Technical Report
TS  Technical Specification
UAV  unmanned aerial vehicle
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>UL</td>
<td>Underwriters Laboratories</td>
</tr>
<tr>
<td>WTO</td>
<td>World Trade Organisation</td>
</tr>
</tbody>
</table>
1. **INTRODUCTION**

Working on overcoming the fragmentation of the EU security market and developing pan-European standards and certification schemes is essential to ensuring the market leading position of EU companies, and to enable the EU industry to meet the security challenges of the twenty-first century more effectively. The fragmentation, currently found throughout the EU, and the situation of divergent national standards are preventing the creation of an “internal market for security, thus hindering the competitiveness of EU industry”.¹

At the European level there is no single framework that applies to security products or the market for security products as a whole at present. Rather there currently exist a ‘multitude of different rules and regulations that have been adopted to cover security concerns related to different sectors, (activities and purposes)’.² Therefore, the European Commission has stressed that addressing this situation in the security sector at national and EU level is one of its most pressing priorities.³⁴⁵

The European Commission has stated that pan-European frameworks for different security areas are required in order to meet the Commission policy objectives, specifically, “avoiding a proliferation of various overlapping and heterogeneous security standards, to arrive at EU-wide standards for the benefit of the internal market”.⁶ This position is echoed by ECORYS, who highlights the widespread ‘(a)bsence of common certification systems for security products at a European level and (that) no mechanism of mutual recognition across countries of products certified at a national level (exist)’.⁷ Security organisations increasingly face technical, operational, and human interoperability issues at their geographical and political borders. A vigorous political will to share assets and standards across Europe will empower them in jointly handling the security issues posed by a progressively more interlinked world.⁸

Divergent approaches have effectively led to the creation of at least 28 different security markets, each of them being split into a large number of security sectors.⁹ Therefore, producing pan-European certification schemes, methods of conformity assessment and standardisation models is also an issue identified as significant in the European Commission Action Plan for an innovative and competitive Security Industry.

ECORYS also highlights the slow speed of response and adaptation of certification procedures notably where new security threats require the implementation of new security solutions

---

⁷ ECORYS, op. cit., 2011, p. 18.
and technologies. Moving to greater mutual recognition between countries, increasing transparency of procedures, and improving the level and quality of interaction between approval and certification bodies could raise the efficiency of the system and support EU security technology development.\textsuperscript{10,11}

ECORYS also draws attention to the New Legislative Framework (NLF),\textsuperscript{12} which is described as an example of an EU ‘generic’ approach. ECORYS suggests that, in principle at least, ‘the NLF could form the basis for any future regulatory approach and to set inter alia performance requirements for security products and technologies’.\textsuperscript{13} According to ECORYS, the NLF has yet to be focused on the security domain and mainly to aspects such as protection of health and safety of products. Some categories of security-relevant products are covered by the EU Construction Products Regulation (CPR), which seeks to ‘ensure reliable information on construction products in relation to their performances … offering uniform assessment methods of the performance of construction products’.\textsuperscript{14} Although this regulation follows an NLF approach, as ECORYS notes, it relates more to products ‘typically somewhat removed from the types of threats normally associated to major civil-security concerns’. At the same time, “security-related requirements for products are not handled through an NLF approach”.\textsuperscript{15}

CRISP (Evaluation and Certification Schemes for Security Products) is a three year project (April 2014 – March 2017) that aims to facilitate a harmonised playing field for the European security industry by developing a robust methodology for security product certification. This report is the second deliverable of CRISP’s work package 2 ‘Review of standards, certification and accreditation for security products’ and consists of nine chapters. Its focus is on security standards, certification and accreditation, best practice and lessons learnt.

Theory describes a practice as a conceptualized idea used to solve a problem or realize a goal. Methods with a proven record of success in this regard are referred to as good practices. Therefore, “good” or “best” practices are those that serve as a means for directly accomplishing useful work via economically sustainable methods. Consequently, “good”\textsuperscript{”}/”best” practices are comprised of a) prospective potential for creating value and b) a tool for isolating, directing and utilizing said potential.\textsuperscript{16}

After a short introduction to conformity assessment in chapter 2, chapter 3 illustrates the state of the art in security standards and certification in ten European countries: Austria, Belgium, Germany, France, the Netherlands, Poland, Slovenia, Spain, Sweden and the United Kingdom. Chapter 4 provides selected international examples including Brazil, Canada, India, Israel, Japan and the United States. The following chapters (5 to 7) show pan-European and international security standardisation activities and certification schemes. Chapter 8 provides information on the state of accreditation in the security context, followed by a summary in

\textsuperscript{10} ECORYS, op. cit., 2011, p. 18-19.
\textsuperscript{11} ECORYS, op. cit., 2011, p. 19.
\textsuperscript{13} ECORYS, op. cit., 2011, p. 19.
\textsuperscript{15} ECORYS, op. cit., 2011, p. 19.
chapter 9. While each country of these analyses provided aspects to learn from, specific good practice is only identified in selected countries. Each country report finishes in the same way with a common summary while specific good practice approaches are highlighted in the last chapter.

CRISP’s focus on the assessment of security products, systems and services (PSS) specifically considers four certification dimensions: security, trust, efficiency and (avoidance of) freedom infringements including privacy. Related to the last dimension, several stand-alone certification schemes exist. Therefore, this report also provides several certification examples in the privacy and data protection field. Regarding technical aspects, specific information is given on alarm systems, CCTV systems, security services and civil drones. This is relevant for further activities in CRISP’s work package 4, in which specific certification aspects in these areas are analysed to show the characteristics of the holistic approach in different security contexts.

References


European Commission, “M/487 Programming mandate addressed to CEN, CENELEC and ETSI to establish security standards”, February 2011,


2. **CONFORMITY ASSESSMENT: AN IMPORTANT TOOL FOR MARKET COORDINATION**

**Reasons for conformity assessment**

The benefits of standardisation in improving economic efficiency and providing access to the world markets cannot be achieved without the ability to make reliable measurements and to be able to demonstrate that items conform to the requirements specified in the standards. These are needed for a variety of purposes, including:

- to demonstrate that products, services and systems meet required specifications. They may include requirements specified under domestic or foreign regulations, trade agreements etc.;
- to establish and monitor appropriate requirements for protection of health, safety and the environment;
- to protect consumers through control of unfair trading practices;
- to ensure compatibility and interoperability of components in products and systems;
- to improve trading opportunities by reducing technical barriers to trade and demonstrating compliance with specifications of international standards, technical regulations and commercial specifications;
- to overcome trade barriers.

To meet these purposes, it is vital to understand and implement the conformity assessment (CA) at national, regional and international levels. All stakeholders of a production process and/or service provision may benefit from the use of CA in their activities. Schematically, it can be shown as following:

![Benefits of conformity assessment to main groups of stakeholders](source)

**Source:** Own figure

**Figure 1:** Benefits of conformity assessment to main groups of stakeholders
Basic characteristics of conformity assessment

In general, CA is defined as the process for demonstrating that different features like quality, safety, reliability, interoperability, meet the requirements of standards, regulations and other specifications. In other words, CA helps to ensure that products, systems and services deliver on their promises.

The International Standardisation Organisation (ISO) and the International Electrotechnical Committee (IEC) define CA in the standard ISO/IEC 17000 as “demonstration that specified requirements relating to a product, process, system, person or body are fulfilled”. Here, the specified requirements include “those contained in suppliers’ or purchasers’ specifications, national, regional or international standards or governmental regulations.” Accreditation of conformity assessment bodies (CABs) is included within the definition of CA.

Several methods can be used for CA including testing, inspection, suppliers' declarations of conformity and certification. Testing includes the related activities of calibration and measurement. Certification includes management systems, product and personnel certification. ISO/IEC 17000, however, does not define the boundaries of CA. These remain elastic.

A possible provider of conformity assessment is

- a person or organisation that provides the object which is being assessed (1st party)
- a person or organisation that has a user interface in the object (2nd party)
- a person or body that is independent of the person or organisation that provides the object and of user interests in the object (3rd party).

One of the basic principles of CA is that the organisation which owns the object of assessment or places it on the market has the primary responsibility for its conformity with the stated requirements.

Conformity assessment and the influence of standards

In the context of the CA there are two major aspects of standardisation to be addressed:

1. availability of national, regional and international standards for setting the requirements for an object and assessing its conformity within them. The term object is used in ISO/IEC 17000 to refer to “product, process, system, person or body”. Conformity with a standard must not be dependent on a particular form of assessment such as certification or accreditation.

2. availability of standards which set out requirements for best practice of CA and the bodies which carry it out. These standards are intended to ensure that there are consistent and internationally harmonized practices among CABs and the bodies with which they work, such as accreditation bodies. The responsibility of these CA standards lies with ISO/CASCO.

ISO/CASCO is the ISO committee on CA which reports to the ISO council and has under its

---

responsibility study of means for assessing the conformity of objects, preparation of standards and guides and promotion of the mutual recognition and acceptance of national and regional assessment systems and the appropriate use of International Standards for testing, inspection, certification, assessment and related purposes.

**Conformity assessment procedures**

One of the characteristics of conformity is that it can take on different forms, using different techniques according to the purposes for which it is being used.

ISO/IEC 17000\(^\text{19}\) proposes a functional approach to CA. Schematically it could be shown as in the following figure.

![Diagram of Conformity Assessment Process](image)

Source: Own figure

**Figure 2: Functional approach to conformity assessment**

**Selection**

The need to demonstrate the fulfillment of specified requirements could be a trigger to start the selection process. The items to be selected are specifications of the standards or other document(s) to which conformity to be addressed, the examples of the object to be assessed or specification of statistical sampling techniques if applicable.

**Determination**

Information on selected items can be represented by specified characteristics of the object of assessment, physical features of the object of the assessment, systems and records relating to the object of assessment, qualities of object, specifications and drawings for the object of assessment. This information is to be tested and evaluated to provide information on fulfillment of special requirements.

**Review and attestation**

During this process the evidence collected from the determination stage is to be reviewed as to the conformity of the object with the specified requirements. Here, there is an opportunity to refer back to the determination stage to resolve nonconformities. Fulfillment of the specified requirements demonstrated can be confirmed by drawing up and issuing a statement of conformity, placing a mark of conformity on conforming products.

---

Surveillance

Surveillance can take place at the point of production or in the supply chain to the marketplace, in the marketplace, at the place of use. Based on the reviewing of the outcome of the determination activities, the referring back to the determination stage may take place to resolve nonconformities. In all other situations this process will end up by drawing up and issuing confirmation of continued conformity.

Conformity assessment schemes, systems and techniques

While each CA situation could be treated differently, there are many advantages of a systematic approach. The basic building block is a scheme which relates to a particular group of objects having sufficiently similar characteristics that the same set of rules and procedures can be carried out under the same management for assessing conformity with the same set of specified requirements.

CA schemes can be set up for commercial purposes, where there is no legal requirement to use such schemes, or for specific CA arrangements required by regulatory authorities to provide assurance that legal requirements are being met. Most CA schemes will be developed by and used in a particular sector of industry or commerce.

Each CA scheme has an owner.20 One of the basic principles of CA is that the organisation which owns the object of assessment or places it on the market has the primary responsibility for its conformity with the stated requirements. A number of different arrangements could apply. Here are some examples:

- a manufacturing organisation;
- a certification body (CB) for sole use of its clients;
- an organisation such as a regulatory body or a trade association which could invite one or more CBs to operate it;
- a group of CBs, perhaps in different countries.

In the third case, in which the scheme owner is an organisation that allows others to operate it, the scheme owner would take responsibility for the operation of the scheme, probably through a contract or other formal agreement with the CBs.

In case that the scheme owner is a group of CBs, it would be necessary for them, as joint owners of the scheme, to create a management structure so that the scheme could be operated effectively by all participating bodies.

It was found necessary to operate several schemes which used same rules, procedures and management, the scheme owner could set up a product certification system under which the different schemes could operate without the need for replicating the management structure for each scheme. In that case, the scheme owner would become the system owner and be responsible for the management of the system and the schemes operating within it.

---

20 More information is provided at ISO, op. cit., 2010, p. 49ff
References


3. European Country Studies

3.1. Austria

3.1.1. Introduction

In the following sections, the Austrian security standardisation and certification sector will be described, by choosing a twofold approach. On the one hand the security standardisation and certification in, nationally and internationally, important institutions and bodies will be described, looking at what security related certifications they provide and also perform and if there are gaps (and where). On the other hand a description of the work at the specific security certification bodies will also provide insight if the gaps left by the important certification bodies can be covered by those security related bodies. Interviews and questionnaires with members and employees of the standardisation institute and certification bodies will help to complement the publicly available information, in order to provide a good analysis of the current security standardisation and certification in Austria.

3.1.2. Short Description of Austria’s Security Industry

As in other countries, the Austrian security industry is very diverse and can be divided into producers of, although mostly not exclusively, security equipment and providers of security PSS. Emphasis has been placed on homeland security, transportation and critical infrastructure protection.21 The estimated total Austrian market demand for safety and security equipment in 2011 was $421.6 million.22 The Austrian statistical office (Statistik Austria) provides statistical data on the Austrian economy in general, dividing the different economic activities according to the Eurostat NACE Rev. 2.23 For statistical data on providers of security solutions, there is a section called “security and investigation activities”.24 The latest register based census of 2011 on the businesses in Austria gives the numbers shown in Figure 3.

The general trend observable for the security services is that the more populated states (Vienna, Lower Austria, Upper Austria and Styria) also have the highest numbers of companies. Furthermore, roughly two third of the security services are private security activities in general, while the other third consists of investigation activities. The security system services are private monitoring centres with intruder alarm connections. These numbers also correlate with a 2010-2011 survey conducted and published by the confederation of European security services (CoESS) on the monitoring and alarm receiving centres in Europe. This survey25 gives also information about the number of connections, received alarms, false alarms, fire connection, etc. in Austria, which are shown in Figure 4.

---

24 NACE Rev. 2 – Statistical classification of economic activities in the European Community p. 82.
Önace 2008

<table>
<thead>
<tr>
<th>State</th>
<th>Private security activities &lt;N801&gt;</th>
<th>Security systems service activities &lt;N802&gt;</th>
<th>Investigation activities &lt;N803&gt;</th>
<th>Σ Security and investigation activities &lt;N80&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burgenland</td>
<td>17</td>
<td>1</td>
<td>19</td>
<td>37</td>
</tr>
<tr>
<td>Kärnten</td>
<td>25</td>
<td>-</td>
<td>11</td>
<td>36</td>
</tr>
<tr>
<td>Niederösterreich</td>
<td>94</td>
<td>1</td>
<td>33</td>
<td>128</td>
</tr>
<tr>
<td>Oberösterreich</td>
<td>51</td>
<td>4</td>
<td>22</td>
<td>77</td>
</tr>
<tr>
<td>Salzburg</td>
<td>35</td>
<td>2</td>
<td>13</td>
<td>50</td>
</tr>
<tr>
<td>Steiermark</td>
<td>81</td>
<td>4</td>
<td>19</td>
<td>104</td>
</tr>
<tr>
<td>Tirol</td>
<td>43</td>
<td>1</td>
<td>19</td>
<td>63</td>
</tr>
<tr>
<td>Vorarlberg</td>
<td>20</td>
<td>-</td>
<td>4</td>
<td>24</td>
</tr>
<tr>
<td>Wien</td>
<td>138</td>
<td>7</td>
<td>53</td>
<td>198</td>
</tr>
<tr>
<td>Total</td>
<td>504</td>
<td>20</td>
<td>193</td>
<td>717</td>
</tr>
</tbody>
</table>

Source: STATcube – Statistische Datenbank from STATISTIK AUSTRIA, data of 2011

Figure 3: Number of security and investigation companies in Austria per state

Number of private monitoring centres that receive intruder alarm connections | 20
Number of private monitoring centre connections<sup>26</sup> | 70,000
Number of private monitoring centre intrusion connections | 50,000
Number of alerts received by the private monitoring centres<sup>27</sup> | 800,000
Number of activations passed to the police from private monitoring centres | 120,000
Annual fee received by private monitoring centres per intrusion connection | 180 €
Number of fire connections<sup>28</sup> | 2,000
Number of technical connections<sup>29</sup> | 12,000
Number of social alarm connections<sup>30</sup> | 10,000
Number of vehicle tracking and tracing connections | 500
Number of e-guarding connections<sup>31</sup> | 70
Number of detector-activated CCTV systems | 500

Source: Statistics from CoESS<sup>32</sup>, data for 2010-2011

Figure 4: Monitoring and alarm receiving centres in Austria

Before the introduction of the EN 50518 Monitoring and alarm receiving centre by CLC technical committee (TC) 79 Alarm systems, CoESS analysed the work of alarm receiving centres in Europe. Compared to the data available from the other countries it is interesting to see that Austrian private monitoring centres pass 15% of the received alarms on to the police. In countries with a similar amount of received alarms, those numbers are much lower (e.g. Italy: 9,000 forwards on 480,000 received alarms (1.88%); Sweden: 45,000 forwards on 1,000,000

---

<sup>26</sup> Number of total connections for all private monitoring centres, including intrusion, social, technical and vehicle tracking for security/safety purposes. Those connections require a human intervention.
<sup>27</sup> Number of alerts received over one year.
<sup>28</sup> The number of fire connections is separate from the other connections.
<sup>29</sup> Separate connections for lift alarms and the like.
<sup>30</sup> E.g. elderly care alarms.
<sup>31</sup> Guarding using CCTV without a trigger.
<sup>32</sup> CoESS, op. cit., 2011.
received alarms (4.5%); Romania: 2,648 forwards on 1,248,312 received alarms (0.21%); Switzerland: 11,000 forwards on 1,400,000 received alarms (0.79%). Also countries with a higher amount of received alarms do not forward as many alarms as Austria to the police (e.g. Netherlands: 45,000 forwards on 5,500,000 received alarms (0.82%); United Kingdom: 251,882 forwards on 6,000,000 to 10,000,000 received alarms (2.52-4.20%)). Only Turkish private monitoring centres, with 449,000 forwards on 1,123,000 received alarms (40%), exceeds the amount of Austrian monitoring centres. Especially the large gap between Austria and the other European countries, ranging between below zero to 4.5% and which seems to be a general practice, is worthwhile noting. These results highlight different security service practices in Europe’s Member States. Based on the introduction of EN 50518 in 2010, further comparisons of the current situation in EU Member States are recommended.

Regarding the security transport industry, representing the secure transport of valuables and cash-in-transit, in 2007 there were three registered companies with a total personnel of 600 and 200 vehicles in Austria. More recent statistical data is unfortunately not available.

The Austrian security research programme KIRAS plays an important role for the Austrian research industry. KIRAS was launched in 2005 and is thus the first national security research programme in the European Union. Financed by the Austrian Ministry for Transport, Innovation and Technology (Bundesministerium für Verkehr, Innovation und Technologie – BMVIT), the objective of the security research programme is to ensure a high level of security for all the members of society in Austria through the security research community. Each project consortium has to be composed by four partners from industry, end-user, research institution and social sciences and humanities. KIRAS provides a security research map of Austria, mapping the individual partners that have participated in the research programme so far. With this map it is possible to identify industry partners which have at least a focus on or are interested in security research. The 206 industry partners range from small and medium-sized enterprises to large businesses like Siemens or G4S.

The Austrian Defence & Security Industry syndicate (ARGE Sicherheit und Wirtschaft) supervises Austrian companies operating in the field of security and especially provides help regarding international und multilateral relations, thus representing the export orientated security industry. In a recent press release from the Austrian Defence & Security Industry syndicate, the importance of the export for the security industry was stressed, especially since the local demand is not able to sustain the industry. With a turnover of roughly € 2.5 bn, the export quota of the (production) industry is at 95%. € 1,858 million were generated in 2010 on the export of measuring, testing and controlling equipment.

---

For the private security services, the CoESS facts and figures 2011 on private security services\(^{39}\) provides further information on the security sector in Austria. The turnover of € 350 million in 2010 from security services can be segmented into general guarding (€ 281 million) being the largest sector, airport security (€ 35 million), cash-in-transit (€ 30 million) and monitoring and remote surveillance (€ 4 million. The Market growth has been constant throughout the last years with peaks in 2004 (22.46%), 2005 (11%) and 2008 (12% compared to the previous year).\(^{40}\)

Security guards in Austria are not required to obtain a license and there is also no specific legislation for the private security services. Currently, the sector is covered by the §129 and §130 of the Trade, Commerce and Industry Regulation Act 1994.\(^{41}\) Basic training of 7.5 hours is necessary and is provided by the Security Academy of the Ministry of the Interior\(^{42}\) and the industry/employers association (Verband der Sicherheitsunternehmen Österreich, VSÖ). Specialised training is required, depending on the security activity. The training intensity is a 7.5 hours course for all, except airport security, where 100 hours of training is foreseen.\(^{43}\)

Finally, on a more political basis the current controversy in Austria concerns private security services handling sovereign duties. In 2013, for the first time in Austria, security at a centre for immigrants in custody pending deportation was outsourced and a big private security service company, “G4S” won the contract to run that centre. Already during the tender by the Austrian Ministry of Interior, criticism emerged due to the outsourcing of security related tasks, upon which the ministry replied that only administration and maintenance tasks, like cleaning and cooking, or the library service would be handled by the company, while the security services would remain under responsibility of the police. However, this was only partly true, as G4S statement and a disclosed operational concept revealed that security services were also meant to be provided.\(^{44,45,46}\)

The main public discussion resulting from this case is thus to what extent sovereign duties should be outsourced by the government, in which even the Austrian liberal political party (NEOS) warns not to subcontract carelessly tasks which affect human rights\(^{47}\) and also the


\(^{40}\) Confederation of European Security Services (CoESS), op. cit., 2011. p. 11.


\(^{43}\) Confederation of European Security Services (CoESS), op. cit., 2011, p. 12f.

\(^{44}\) Criteria regarding the staff of the bidder for the tender are for example at least 150 staff members with a ÖZS (Österreich Zertifizierungsstelle Sicherheit; Austrian Security Certification Body) certified basis training and the bidding company needs to be a certified ÖZS Security Service Company with a ÖZS certified alarm receiving center.


\(^{47}\) NEOS, op. cit., 29.10.2014.
opinion of the media is more sceptical than the governmental opinion.\textsuperscript{48} The revelations by the “Guardian” and other newspapers about grievances and possible human rights violations in prisons and services run by G4S\textsuperscript{49} also strengthened opposition against the planned implementation of a private security company. The contract between G4S and the Austrian Ministry of Interior is set for 15 year and started on the 15\textsuperscript{th} January 2014, leaving the opponents of the project in the role of the supervisors.

### 3.1.3. The Security Standardisation Framework

Responsible for the standardisations in Austria is the “Austrian Standardisation Institute” (ASI), with their main product being the publication of Austrian Standards (ÖNORM), either developed upon the initiative of stakeholders or taken over as national standards within the framework of European and international standardisation. The ASI was founded as the “Austrian Standards Committee for Industry and Commerce” (Österreichischer Normenausschuss für Industrie und Gewerbe - Ö.N.I.G.) in 1920 and published their first ÖNORM in 1921. At the end of 2013 the total number of documents available by the ASI reached 24,730. Besides the ÖNORMs (including the ones based on European and international standards) the ASI also publishes ON rules (ONR) which are similar to the workshop agreements or the publicly available specifications at the international level. The ASI is legally regulated by the Standardisation Act of 1971 (Normengesetz of 1971).\textsuperscript{50}

Although a large amount of security-related ÖNORM documents exist, specific security committees are scarce at the ASI. Relevant TCs are dispersed in different subject fields, for example in the safety field, traffic & transport field, services & management field or in the environment field. Examples of relevant security TCs are the committee 246 societal security, a mirror committee of the societal security committees at CEN (TC 391 Societal and citizen security) and ISO (TC 223 Societal security) in which the ASI is also a member (see also Figure 5),\textsuperscript{51} the committee 252 on risk management, business continuity management and corporate security management,\textsuperscript{52} or the committees 041 on fire service equipment and fire protection\textsuperscript{53} and 172 on automatic fire fighting systems.\textsuperscript{54} Since CRISP partners had the opportunity to talk with the managers of those committees, interesting aspects emerged, which will be presented here.


\textsuperscript{51} Austrian Standardisation Institute, Committee 246, 2014, https://committees.austrian-standards.at/detail/8620.

\textsuperscript{52} Austrian Standardisation Institute, Committee 252, 2014, https://committees.austrian-standards.at/detail/16410.

\textsuperscript{53} Austrian Standardisation Institute, Committee 041, 2014, https://committees.austrian-standards.at/detail/181.

\textsuperscript{54} Austrian Standardisation Institute, Committee 172, 2014, https://committees.austrian-standards.at/committee/show?id=862&locale=en
While some of the developed standards by those committees are the result of the implementation of European and international standards, a lot of national standards are developed as well, primarily as a result of the needs of national stakeholders. For example national standards of the committee 041 on fire service equipment and fire protection have the label “ÖNORM F” (the “F” stands for fire protection and fire services), of which 42 standards (and draft standards) are in use. The most prominent and interesting standard-series is on automatic fire alarm systems – which have no real equivalent on the European level. Although European standards on fire alarm systems (EN 54-2) exist, ASI has developed more specific standards here, like e.g. the “ÖNORM F 3070:2010 – Planning, development, installation, commissioning and maintenance of fire detection and fire alarm systems and of fire control devices”.\(^{55}\) But also the “ÖNORM F 3000:1989 – fire alarm systems”\(^{56}\) of the committee 172 on automatic fire fighting systems should be mentioned here – as this standard is often a requirement within public procurement tenders. Currently this standard is being updated by the committee 172.

For the committee 252 on risk management, national standards are labelled “ÖNORM S” (the “S” stands for “sonstige Normungsgebiete” – other standardisation areas), of which currently seven exist – the “ÖNORM S 2400” series on “Business Continuity und Corporate Security Management”.\(^{57}\)

Other ASI TCs have only partly a focus on security related standards which are worth mentioning here.\(^{58}\) Those include the committees information technology (mainly the working groups IT-Security and biometrics), water supply (with standards on the security of water supply in crisis situations) and in the area of crisis management the committee on the protection of natural hazards. Most of those TCs have also a mirror committee at the European and international standardisation bodies.

Figure 5 shows a selection of ISO TCs with a focus on security topics, based on the description of the work of international standardisation organisations in the CRISP deliverable 2.1.\(^{59}\) The work of all relevant TCs is described in detail in chapter 5.

The figure shows that the Austrian standardisation institute participates in most of the security related TCs (although in some only as observation member) except for the specific security TC. Some of those TCs can also be found as TCs at the ASI, as shown above.


\(^{58}\) A complete list of technical committees can be found here: Austrian Standardisation Institute, Standardization committees by number and working groups, 2014, https://committees.austrian-standards.at/numbers?locale=en.

At European level, ASI also participates in some relevant TCs, as for example the CEN TC 192 on Fire and rescue service equipment, the CEN/TC 164/WG 15 on the Security of drinking water supply or the CEN TC 391 Societal and citizen security. Furthermore, the ASI held the secretary of the CEN TC 384 on Airport and aviation security and holds now the secretary of the CEN TC 417 on Maritime and port security. Currently in discussion is to sum the results of the airport, maritime and port security, and other security service TCs into a new TC on private security services.

The standardisation of security services in Austria is also currently in an ongoing discussion, although still at an early stage. The legal regulation of security services is dealt with in the Trade, Commerce and Industry Regulation Act 1994 – and thus within the scope of the federal ministry of science, research and economy. Since the security services have started to operate more and more in the field of the executive forces, considerations are to implement the legal regulations of security services within the federal ministry of interior. Another possibility that is also being discussed is to create national standards for the qualification of security service personnel. The current problem is, although not only, the regulation of the security

---

60 For more information about the TC 417 on maritime and port security see Wurster, Simone, et al., op. cit., 2014, p. 88f.
services in the Trade, Commerce and Industry Regulation Act but also that for some part duties of security services – e.g. for event-security – are regulated in different federal state laws. So several legal frameworks have to be considered for security services, but show also the necessity of changes within the current regulatory format.

The role of the Austrian standardisation institute regarding security standardisations is important and reflects nicely the interplay between national and supranational standardisation institutes – with the ASI adapting the requirements set on the European and international level to needs of the Austrian industry and end-users. This can be seen in specific standards, as for example standards for the protection of natural hazards – mainly relating to avalanches and flooding – an Austrian/alpine specific threat, but also with the newly emerged discussion about the implementation of security services in standardisation.

### 3.1.4. The Security Conformity Assessment Framework

At the Austrian standardisation institute, the committee 253 on conformity assessment deals with the standardisation of requirements for accreditation bodies, for testing, inspection and certification bodies, of procedures for evaluation of conformity in the field of testing and certification and of terminology in the field of evaluation of conformity. The TC 253 thus represents the CEN/CLC TC 001 Criteria for conformity assessment bodies and the ISO TC CASCO Committee on conformity assessment on the national level. Furthermore, the agendas of the IEC CAB and the Senior Officials Group for Standardisation and Conformity Assessment Policy (SOGS) are also integrated into the national work of the committee. The developed documents of the conformity assessment committee are all based on the EN and ISO documents from the before mentioned committees, and thus an implementation of the international standards on the national level.

For certifications and audits of security PSS, important standards here are for example the ÖVE/ÖNORM EN ISO/IEC 17021:2011 Conformity assessment - Requirements for bodies providing audit and certification of management systems, setting requirements for audits of information security management systems and the like. Currently a new version of this standard is being developed and a draft version has already been released on the 15th September 2014. Similar standards also exist for product, process and service certifications.

The regulation (EC) No 765/2008 of the European parliament and council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products\(^ {62}\) and the Austrian Accreditation Law (Bundesgesetz über die Akkreditierung von Konformitätsbewertungsstellen, AkkG)\(^ {63}\) are two important legal documents, not only for the committee 253 on conformity assessment but also for the accreditation and certification in general. With the implementation of the AkkG, the Austrian Federal Ministry of Science, Research and Economy (Bundesministerium für Wissenschaft, Forschung und Wirtschaft,

---

\(^{61}\) Those standards have of course a broad focus and do not solely set requirements for the certification of products, processes, systems and services.


BMWF) has been assigned with the accreditation of conformity assessment bodies which are based in Austria. A close cooperation between the ASI – committee 253 and the accreditation of the BMWF (also called Akkreditierung Austria) grants the development of the conformity assessment standards. Akkreditierung Austria is also a member of the European cooperation for Accreditation (EA) and thus guarantees the equalisation of Austrian conformity assessment bodies with other European countries.

In total 458 conformity assessment bodies are accredited by the Akkreditierung Austria, of which 75 are in the field of certification:

- 39 are certification bodies for products,
- 15 certification bodies for management-systems,
- 17 certification bodies for persons and
- 4 verification bodies.

For the current analysis of certification bodies in Austria with a focus on security products, systems and/or services, nine private certification bodies have been identified as relevant, through the publicly available information:

- Austrian Standards Institute – Certification
- Bureau Veritas
- Certification Information Security
- Lloyd's Register Quality Assurance
- Quality-Austria
- SGS Group Austria
- TÜV Austria
- TÜV Süd Austria
- Wifi (Wirtschaftsförderungsinstitut) Österreich – Zertifizierung

Based on the results of the CRISP deliverable 2.1, especially of the interviews with relevant security CEN/CLC TCs, the use of specific standards for certification has been identified. Seventeen standards are relevant in this regard. In Figure 6, these standards have been listed with their usage in certifications in Austria, including the performing conformity assessment body. From those standards, only eight are offered by accredited organisations.

---


66 Since these accredited certification bodies were also contacted for further information regarding their work in the security certification, a detailed description of those bodies is provided in the section “Selected security certification bodies and their work.”

67 Wurster, Simone, et al., op. cit., 2014
<table>
<thead>
<tr>
<th>Standard</th>
<th>Σ Accredited CABs(^{68})</th>
<th>Names of the CABs</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 28000 series</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>ISO/IEC 27000</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>IEC 62443</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>IEC 62642</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>EN ISO 22301</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>EN ISO 27799</td>
<td>1</td>
<td>TÜV Austria Services GmbH(^{69})</td>
</tr>
<tr>
<td>EN 13094</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>EN 14025</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>EN 12972</td>
<td>1</td>
<td>TÜV Austria Services GmbH(^{70})</td>
</tr>
<tr>
<td>EN 14339</td>
<td>2</td>
<td>Austrian Institute of Technology, Standort Giefinggasse, OFI Technologie Innovation GmbH(^{71})</td>
</tr>
<tr>
<td>EN 14384</td>
<td>2</td>
<td>Austrian Institute of Technology, Standort Giefinggasse, OFI Technologie &amp; Innovation GmbH</td>
</tr>
<tr>
<td>EN 50131</td>
<td>1</td>
<td>OVE Österreichischer Verband für Elektrotechnik</td>
</tr>
<tr>
<td>EN 50133</td>
<td>1</td>
<td>OVE Österreichischer Verband für Elektrotechnik</td>
</tr>
<tr>
<td>EN 50136</td>
<td>1</td>
<td>OVE Österreichischer Verband für Elektrotechnik</td>
</tr>
<tr>
<td>EN 50518</td>
<td>2</td>
<td>OVE Österreichischer Verband für Elektrotechnik, TÜV Austria Cert GmbH</td>
</tr>
<tr>
<td>EN 54 series</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>EN 62676</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Source: Own figure, Austrian Federal Ministry of Science, Research and Economy

Figure 6: Selected standards as a basis for certification in Austria

Beside the accredited conformity assessment bodies (CABs), there are two other, non-accredited CABs interesting for this country study, which are also intertwined: The “Verband der Sicherheitsunternehmen Österreichs” (VSÖ; Austrian Association of Security Companies) and the “Österreichische Zertifizierungsstelle Sicherheit” (ÖZS; Austrian Certification Body Security). Both have a strong (and only) focus on security – of products as well as services – and thus offer the broadest range of certifications in this area and therefore their importance in the security industry is unquestionable.

---

68 Conformity Assessment Bodies
69 accredited as inspection body - ISO/IEC 17020
70 accredited as testing body - ISO/IEC 17025
71 accredited as testing body - ISO/IEC 17025
72 accredited as inspection body - ISO/IEC 17020 & Certification body for products - ISO/IEC 17065
3.1.5. **SELECTED SECURITY CERTIFICATION BODIES AND THEIR WORK**

For the certification bodies related to security in Austria, we have contacted several institutions in order to identify the certification process and the related work. The contacted certification bodies are listed in the Figure 7. The selection of the certification bodies was based on the previous research of the security industry and the accreditation of conformity assessment bodies in Austria.

The contacted certification bodies represent on the one hand the most important general certification bodies in Austria – where also some kind of security related certification could be expected and on the other hand, the most important ones with a specific focus on security. Unfortunately, not every certification body replied to CRISP’s requests, including the more important certification bodies with a strong focus on security.

<table>
<thead>
<tr>
<th>Certification of:</th>
<th>Security products</th>
<th>Security systems</th>
<th>Security services</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Body:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Austrian Standards Institute – Certification</td>
<td></td>
<td></td>
<td>X (Personnel)</td>
<td></td>
</tr>
<tr>
<td>Bureau Veritas</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certification Information Security</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lloyd's Register Quality Assurance</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality Austria</td>
<td>X</td>
<td>X (Personnel)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SGS Group Austria</td>
<td>X</td>
<td>X (Personnel)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TUV Austria</td>
<td>X</td>
<td></td>
<td>(Rarely)</td>
<td></td>
</tr>
<tr>
<td>TUV Süd Austria</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wifi (Wirtschaftsförderungsinstitut) Österreich - Zertifizierung</td>
<td>X</td>
<td></td>
<td>X (Personnel)</td>
<td></td>
</tr>
<tr>
<td>Österreichische Zertifizierungsstelle Sicherheit</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Verband der Sicherheitsunternehmen Österreich (VSÖ)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Source: Own figure
Figure 7: Overview of important (security) certification bodies in Austria

The following detailed description of the security certification bodies is based on the information available online and, where available by the information they provided CRISP by e-mail and phone.

**Austrian Standards Institute – Certification**

The Austrian Standards Institute (ASI) is – as described above – the national standardisation body. Beside the development of standards, they also run an independent, accredited certification branch, called the Austrian Standards Plus Ltd.\(^73\) ASI mainly performs certifications for (construction-) products – primarily for the Austrian market, but also for the international market, as well as service and system certifications. Beside those areas, ASI also provides

---

personnel certification, in which individuals can be certified for example as an “ON Certified Person” for risk management, amongst others.\footnote{Austrian Standards, “Personal Certification”, 2014. \url{https://www.austrian-standards.at/en/products-services/certification/personal-certification/}}

The risk management certification can be obtained by persons having finished a minimum 40 hours training for risk managers based on the ONR 49003 “Risk Management for Organizations and Systems”.\footnote{Austrian Standards Institute, “ONR 49003 Risk Management for Organizations and Systems, Requirements for the qualification of the Risk Manager, Implementation of ISO 31000”, 01.01.2014.} The ONR 49003 is the implementation of the international ISO 31000 family on risk management in Austria and describes the requirements for the training/qualification of risk managers. This qualifies a person to work for example as an (internal or external expert) in security management, or in emergency, crisis and business continuity management. This is the only certification in the field of security being provided by the ASI.

**Bureau Veritas**

Bureau Veritas is one of the leading testing and certification providers in the world, with their main office in Paris, France, providing certifications in more than 140 countries. They provide a wide range of services, like health, safety an environment services for industrial sites, personal training and qualifications (e.g. for risk management) and also certifications as an accredited certifier.

Bureau Veritas Austria provides specific security certifications for logistics and transportation security, based on international standards. There are three certifications available, each responsible for specific areas in the logistics chain while still being intertwined:

- **ISO/PAS 28000:2007** - Specification for security management systems for the supply chain certifications. The ISO 28000 sets the requirements for security management systems in supply chains, Bureau Veritas provides the audit of the correct implementation of the standard and helps – through re-certifications – on the optimisation of the different areas of security management systems.\footnote{Bureau Veritas Certification Services, “ISO/PAS 28000 certification”, no date. \url{http://www.bureauveritas.de/wps/wcm/connect/a5e06cd4-5b58-4e3d-a476-99f17862b0c/FS+ISO+28000.pdf?MOD=AJPERES.}}

- **TAPA Certification**: TAPA is the acronym of the Transport Asset Protection Association, an association of technology industrials, settings standards to secure the whole logistics and supply chain against thefts in all the areas of the transport (air, land and water). TAPA develops own standards aiming at this specific problem, called Freight Security Requirements (FSR), which set the minimum acceptable security standards. The certification of the TAPA FSRs includes the different sectors of the logistics, including the security areas, access control, offices, storehouses, security systems and instructions, early warning systems and advanced security requirements.\footnote{Bureau Veritas Certification Services, “TAPA Zertifizierung”, no date. \url{http://www.bureauveritas.de/wps/wcm/connect/35c9ef89-d446-4af6-b40b-f3226a35a013/FS+TAPA.pdf?MOD=AJPERES.}}
• Certification of Transport logistics: Integrated management systems for haulier, transport, transhipment and storing. This certification is mainly based on the ISO 9001 and thus not really security related, but it is easily combined with the TAPA certification.78

Information about the specific functioning and demand of those certifications would have been interesting, but unfortunately Bureau Veritas Austria has so far not responded to interview requests, which is why no specific information can be provided here. It would have been especially interesting for Austrian specifications. Due to the location in central Europe with connection to the eastern European countries, Austria has become an important (transit) country in terms of freight traffic since 2004, which has led to an increase in traffic, including the corresponding (security) problems.

Certification & Information Security Service (CIS)

CIS – Certification and Information security service ltd. is a Vienna based certification body, specialising on certification in information security according to ISO/IEC 27001 and IT service management according to ISO/IEC 20000, and is accredited by the Federal Ministry of Science, Research and Economy. Beside the abovementioned certifications, CIS also provides courses for individuals based on these international standards.

CIS replies to CRISP’s questionnaire follow below:

<table>
<thead>
<tr>
<th>Kinds of PSS which are tested and certified in the security field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information security management systems (ISMS)</td>
</tr>
<tr>
<td>Information technology service management systems</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Certification process(es) in the security area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information -&gt; CIS-Stage-review (optional) -&gt; CIS-System-and-Risk-Review -&gt; CIS-Certification Audit -&gt; CIS-Certificate (valid 3 years) -&gt; CIS-Surveillance-Audit (Once a year) -&gt; CIS-Recertification-Audit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Documents which form the basis of the testing and certification process(es)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laws/regulations</td>
</tr>
<tr>
<td>Internal guidelines/documents</td>
</tr>
<tr>
<td>Other documents</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security PSS which are certified based on the aforementioned standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product/technology/system/service</td>
</tr>
<tr>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Information security management systems</td>
</tr>
<tr>
<td>Information technology service management system</td>
</tr>
</tbody>
</table>

Quality seal

Key evaluation criteria in the security field and requirements for obtaining a certificate

<table>
<thead>
<tr>
<th>Product/technology/system/service: ISMS</th>
<th>Evaluation criterion</th>
<th>Minimum requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk-analysis, Statement of application, contents of the ISO 27001</td>
<td>Minimum requirements as set by the ISO 27001</td>
<td></td>
</tr>
</tbody>
</table>

Cooperation with external test laboratories in the security field

None

Involvement of the organisation in security standardisation

Austrian Standards AG 001.27 (IT Security) – the national committee of the development of ISO 27XXX and other IT security standards.

Number of certificates issued in the security field annually

No Information

(Mutual recognition) agreements with other European countries/certification bodies in the security field

None

Solutions for suppliers of certified security solutions from other European countries that wish to receive a certificate that is valid in the country

CIS operates in 30 countries, as a partner or with an own branch.  

Summary

Especially regarding the ISMS certification, there is an increase of demand.

Lloyd's Register Quality Assurance

Lloyd’s Register Quality Assurance (LRQA) is a certification body similar to Bureau Veritas, being an international provider of certifications in different sectors. LRQA is a London based company and a 100% subsidiary of Lloyd’s Register Group Ltd. LRQA is an accredited certifier in 30 countries, including, for example, Austria. Regarding security certifications, Lloyd’s provides, again similar to Bureau Veritas, certifications of management systems in supply

---

chain security, mainly based on the ISO/PAS 28000, and – similar to CIS – certifications IT security services and management systems (based on ISO/IEC 20000-1 and ISO/IEC 27001). Regarding the certification of supply chain services, the ISO 28000 also considers the different existing supply chain regulations, for example the TAPA freight security requirements. Unfortunately, LRQA also failed to reply on CRISP’s interview request, which is why a more specific description of this certification body’s work cannot be provided here.

Quality-Austria

Another accredited certification body in Austria is Quality-Austria, with a broad range of certifications in different areas. Relevant in this context is the certification of risk and security management.\(^{80}\) Certification in this area relies on the ISO 31000 and the Austrian implementation ONR 49001 standard on risk management – as it is also provided by the Austrian Standards Plus. Furthermore, Quality-Austria also offers certifications on the basis of the ISO 22301:2012 standard.\(^{81}\) Upon CRISP’s interview request, the contact at Quality-Austria replied that they currently do not perform any security related certifications, which is why they unfortunately could not provide CRISP with any relevant information.

SGS-Austria

SGS-Austria is an accredited certification body which is part of the worldwide operating SGS-group. SGS-Austria is comparable with Quality-Austria, performing a wide variety of certifications of PSS. In the area of security certifications, SGS-Austria offers ISO 22301 and ISO 31000 based certifications, risk management for enterprises and individuals. Similar to Bureau Veritas and LRQA, certifications for the supply chain security on the basis of the ISO 28000, TAPA Trucking Security Requirements and TAPA Freight Security Requirements standards are also offered by SGS-Austria. Lastly the certification of management system in IT-Security – ISO 27001 – is performed by SGS as well. Again due to the non-responses to CRISP’s interview requests, a more specific description of the work and the certifications by SGS-Austria is not available.

TÜV-Austria

The TÜV-Austria has an expertise of more than 140 years\(^{82}\) as an inspection, control and certification body, operating in over 20 countries, resulting in an important international reputation of the TÜV-Austria certificate. The certification offered by the TÜV-Austria covers the three main areas of products, systems and personal certification. Although TÜV-Austria does not perform a lot of certifications in the field of security, they accepted the interview request. Here some interesting findings emerged, which will be highlighted in the further description of the work of the TÜV-Austria.

---


\(^{82}\) TÜV Austria, “The history of TÜV AUSTRIA Group”, No date, http://www.tuev.at/start/browse/en/Webseiten/TUV%20Austria%20Holding/Wir%20%C3%9Cher%20Uns/Geschichte-des-History-of-T%C3%9CV-AUSTRIA.
The most important part of the security certification is performed in the system certification. This is not as different as in the other above mentioned certification bodies, offering certifications for supply chain security (based on the ISO 28000) or for IT Security management systems (based on the ISO 27001). Personal security-certification is mostly based on Risk management, while the product certifications performed by the TÜV-Austria have no focus on security products, as here they mostly test the technical functioning and thus the safety hazards that could result from the product.

The TÜV-Austria is furthermore accredited to certify monitoring and alarm receiving centres, based on the EN 50518. Here not only the physical structure and the technical functioning of the alarm receiving centres are monitored by the TÜV, but also the day-to-day procedures in the centres are part of the certification. During the interview it was noted that so far there have been no certifications of monitoring and alarm receiving centres. In general, at least for TÜV-Austria, the requests of the stakeholders and thus the interest of the TÜV in security service certifications are not very high. It seems there is not enough demand for certifications in these areas, even though – according to the TÜV-Austria – the standards for these kinds of certifications are available. For example the DIN 77200, used by the German section of the TÜV-Austria. This standard sets requirements for different security services (ranging from guarding, to canine services and assets security), on the one hand regarding the different equipment of the security services and on the other hand setting minimum qualification standards for the employees. Furthermore the standard regulates what tasks are to be performed by the different security services.

The interviewee mentioned that for Austria, this standard could also be considered, if the necessity for security standards emerges and at least at TÜV-Austria, they rely on this standard for the few audits they perform on security services. In general though, according to the interviewee, most of the security service requirements are regulated in Austria anyway on a governmental level. This is, as described already in the section on the security industry in Austria, mainly regulated by the §129 and §130 of the Trade, Commerce and Industry Regulation Act 1994.

At the TÜV-Austria, the main focus isn’t on security certifications and wont probably be in the future, as they mainly perform product certifications and the demand for security certifications (mainly regarding the services), isn’t important enough. There is of course always a discussion, where to improve, but this is also always a matter of resources. Still, the TÜV-Austria showed a great interest in the work of the CRISP consortium as it fits into the different security discussions.

**TÜV Süd Austria**

TÜV Süd Austria is, compared to TÜV-Austria, not a stand-alone certification body, but the Austrian section of the company based in Germany. Accredited by the Federal Ministry of Science, Research and Economy, TÜV Süd Austria performs beside the product certification also the certification of systems and individuals. This results in the security sector having mainly certifications in IT-security, similar to CIS, based on the two important standards ISO 20000 in IT Service Management and ISO 27001 on Information Security Management Sys-

---

83 EN 50518:2013 - Monitoring and alarm receiving centre.
84 DIN 77200 - Sicherungsdienstleistungen.
tems. Certifications are also performed based on the IEC 62443 – Industrial communication networks – Network and system security, as well as on risk analysis and management, both in context of secure city solutions, as “rapid urbanisation and expanding populations pose greater issues for crowd control and need comprehensive evacuation plans in the event of natural or man-made disasters”. The interview request addressed to the TÜV Süd Austria has remained unanswered, which is why also here, a more specific description of security-certificate cannot be provided.

**Wifi (Wirtschaftsförderungsinstitut) Österreich – Zertifizierung**

The “Wirtschaftsförderungsinstitut Österreich” (WIFI) is an adult education institute of the Austrian Federal Economic Chamber (Wirtschaftskammer Österreich – WKÖ), which has also been accredited by the Federal Ministry of Science, Research and Economy as a certification body, with a strong focus on personal certification. Although most of the certifications have a more technical character, the WIFI also issues certificates for (Senior) Risk managers, based on the ÖNORM EN ISO 31000 and the ONR 49003. Beside the risk manager certification, the WIFI had also provided certifications of the qualification of security service personnel, but due to a too low demand, these certifications have been dismissed. Since the WIFI thus does not really offers security certifications, they could not take part in the interview and provide CRISP with supplementary information.

**Österreichische Zertifizierungsstelle Sicherheit**

The “Österreichische Zertifizierungsstelle Sicherheit” (ÖZS – Austrian Certification Body Security) is a certification body specialised on mechanical and electronically security technology, as well as security services. The ÖZS is not accredited by the Federal Ministry of Science, Research and Economy, but is since 2010 also part of the Austrian Electro-technical Association (Österreichischer Verband für Elektrotechnik – ÖVE), which is an accredited certification and inspection body in the field of electro-technology (based on the EN ISO/IEC 17065:2013 -- Certification Body for Products and EN ISO/IEC 17020:2012 -- Inspection Body Type A). The ÖZS issues ÖZS-certificates, based on internal guidelines. Three guidelines are available online – without any further specifications about the scope:

- ÖZS BW2:2008-07-01 ÖZS-Richtlinie für die Zertifizierung von Sicherheitsdienstleistungsunternehmen (ÖZS-guideline on the certification of security services);
- TRVE 38-1: Ausgabe 2, Dezember 2009 Richtlinien für Notrufzentralen mit Intervention; Bauliche, technische und personelle Voraussetzungen (guideline for emergency call-centres; structural, technical and personnel requirements);
- ÖZS RA01:2009-12-01 ÖZS-Richtlinie für die Zertifizierung von Rufanlagen für Krankenhäuser, Pflegeheime und ähnliche Einrichtungen (ÖZS-guideline on the certification for call systems in hospitals, care homes and similar institutions).

---

Especially the first two guidelines appear to be similar to other existing standards which are internationally available, like for example the DIN 77200 – “Anforderungen an Sicherungsdiensleistungen” or the EN 50518:2013 – “Monitoring and alarm receiving centre”. The ÖZS did not reply to CRISP’s interview requests, which is unfortunately, as it would be interesting to know what reasoning behind the development of own guidelines in the area of security standards was. Furthermore interesting – at least regarding the publically available information – is that so far only four security service companies are certified on the basis of the ÖZS BW2:2008-07-01. These four companies are also the four important security service providers in Austria (some also globally), namely G4S Secure Solutions AG, ÖWD Österreichischer Wachdienst GmbH & Co KG, Securitas Sicherheitsdienstleistungen GmbH and Siwacht Bewachungsdienst GmbH. These four companies are also the only ÖZS certified emergency call-centre (TRVE 38-1: Ausgabe 2, Dezember 2009), besides the A1 Telekom Austria AG. Here it would thus also be interesting to know, what criteria are important to obtain these certificates and if it’s on the basis of these criteria that ‘only’ four companies hold these certificates, or what other reasons are behind the limited number of ÖZS certified companies.

Verband der Sicherheitsunternehmen Österreich

The “Verband der Sicherheitsunternehmen Österreich” (VSÖ – Organisation of the Security-companies Austria) is a security stakeholder association, which also sets security standards/guidelines and performs certifications on basis of those standards. The VSÖ closely cooperates with the ÖZS and is not accredited by the Federal Ministry of Science, Research and Economy. Currently the VSÖ holds 46 members divided into three technical units:89

- Electronic security systems (intruder alarm, CCTV and access control systems);
- Mechanic security systems (high-security doors, safes and latches);
- Security services (guard services, event services and alarm system services).

Being a VSÖ member has of course several advantages, be it networking and lobbying or developing standards/guidelines and obtaining certifications based on those guidelines. The developed VSÖ guidelines are mostly technical standards but also set requirements for the operation of the security products and systems. The currently available VSÖ guidelines are:90

- OVE R2: Einbruch- und Überfallmeldeanlagen - Planung, Einbau, Betrieb und Instandhaltung (Burglary- and intrusion alarm system - planning, installation, operation and service);
- OVE R9: Alarmanlagen - CCTV-Überwachungsanlagen für Sicherungsanwendungen. Planung, Einbau, Betrieb und Instandhaltung (Alarm systems - CCTV-surveillance systems for security application. Planning, installation, operation and service);

• TRVE 31-7 Richtlinien für Einbruchmeldeanlagen Planung und Einbau (guidelines for burglary alarm systems – planning and installation);
• TRVE 32-7 Richtlinien für Security Videoüberwachungsanlagen (guideline for security video-surveillance systems);
• TRVE 20-1 Anerkennung von einbruchhemmenden Türen als VSÖ-Hochsicherheitstür (Approval of burglar-resistant doors as VSÖ-High-security doors);
• TRVE 20-2 Anforderungen für die Anerkennung von Montagefirmen für den Einbau von VSÖ Hochsicherheitstüren (Requirements for the approval of installation companies for the installation of VSÖ-High-security doors);
• TRVE 38-1 Richtlinien für Notrufzentralen mit Intervention. Bauliche, technische und personelle Voraussetzungen (guideline for emergency call-centres; structural, technical and personnel requirements).

These standards are developed in cooperation with the ÖVE and are also part of the certifications performed by the ÖZS. Furthermore, the VSÖ recommends the ÖZS personal training for security services (which relates to the ÖZS BW2:2008-07-01 guideline). Again, a more specific description of the work in the area of security certifications is not possible, as the VSÖ did not reply to CRISP’s interview request.

3.1.6. SUMMARY AND CONCLUSION

This case study unveiled interesting aspects in various areas. Austria’s standards for fire alarm systems and fire safety equipment, for example, are often more specific than their European or international counterpart. The Austrian Standards Institute ASI also showed a lot of interest in the CRISP project, which resulted in detailed conversations on the security standardisation in Austria.

Regarding the certification, it can generally be seen that in Austria there are two, closely cooperating organisations responsible for the essential security certifications, which are the “Österreichische Zertifizierungsstelle Sicherheit” (ÖZS) and the “Verband Sicherheitsunternehmen Österreich” (VSÖ). Although both were not available for interviews, some interesting insights on the work of those organisations could be gained through the publically available information. These can be summed into three aspects – important stakeholders as association members, the development of own guidelines, and close internal (amongst members), as well as external (with governmental institutions) cooperation – which we will expound here.

Stakeholders in associations developing guidelines and providing certifications are important, since the development of the guidelines can be closely related to the needs of the industry and also end-users. In the ÖZS, the Österreichischer Verband für Elektrotechnik (ÖVE) and the VSÖ concerning security service companies, the four (or five for the VSÖ) largest companies operating in this field are the only members, being G4S Secure Solutions AG, ÖWD Österreichischer Wachdienst GmbH & Co KG, Securitas Sicherheitsdienstleistungen GmbH, Siwacht Bewachungsdienst GmbH, and Loomis Österreich GmbH (cash transport).91 In this

---

case although, problems might arise where the market leaders of a certain section are the only members – and also represent the head of the technical unit. Especially since the ÖZS and the VSÖ offer a reduced amount of guidelines and are very specified on security products and services, the intertwining of the market-leading stakeholders could have an impact on the impartiality of the standardisation and certification.

The problems which might arise with this, also lead to the second before-mentioned aspect – the development of own guidelines. While in some cases, European and international standards might not, or only partly be available (especially concerning security service qualifications), other of the guidelines developed by the VSÖ, ÖVE and ÖZS are also covered by ENs and ISO standards. The risk of developing own standards, which are especially tailored to fit the members of the association, is not to be neglected. This could on the one hand result in the stabilisation of the market leadership of the large security companies, disadvantage the smaller companies and hinder the development of the market. On the other hand, it also can prevent that small companies want to participate in the discourse and the development of the associations. Although it appears as if the VSÖ would want more members from security service companies, the application for smaller companies is difficult. Not only is the power of the big security companies in the association a symbolic hurdle, but there are also real barriers resulting from the criteria in the – by the VSÖ and ÖZS developed – guidelines. The security company should, for example, be able to employ five times more security personnel as necessary for one assignment, which many small security companies can not afford. Also the implementation of a 24-hours emergency call-centre, as set by the TRVE 38-1 guidelines is not feasible for every security company.94

This also leads to the third and last aspect – the close cooperation, especially with governmental organisations. This can of course be an important aspect of the association, especially since setting the quality requirements of security PSS always leads to an important political and societal discourse – which is part of the CRISP project, where also the trust and freedom infringement parts of security PSS are analysed and how they can be handled in security certifications. But the close cooperation with governmental organisations, combined with the previous two aspects can also lead to scenarios, where governmental tenders can only be won by certain members of the VSÖ, as the requirements of the tender comply with the requirements of VSÖ and ÖZS guidelines, as already described with the tender for the centre for immigrants in custody pending deportation, which was won by the G4S GmbH.95

The VSÖ and ÖZS are two important security certification bodies, as they cover a large part of the security market and it is apparent that they hold a large body of knowledge, also through their close cooperation with the stakeholders. An insight into the work of both would have been very helpful, in order to better understand the reasoning behind the structure – and also the three aspects described above. The controversy of important market-leading stakeholders, apparently setting the criteria of the guidelines, seems also not really in line with the propagated impartiality of standardisation bodies. Other – accredited – certification bodies are

---

93 VSÖ Secretary General Thomas Forstner currently was quoted by the newspaper “Die Presse” in an article dealing with the same problematic: “The more members, the stronger we are. Our goal at the association is after all to raise the quality in the sector and have a legally based qualification for securities.” Winroither, Eva, “Ministerium stützt nur große Securityfirmen”, Die Presse, 16.07.2014, http://diepresse.com/home/panorama/oesterreich/3839697/Ministerium-stutzt-nur-grosse-Securityfirmen.
not as important in the security sector. Some do provide and perform a few certifications which have a security focus, while it seems that amongst those certification bodies, the demand for such certifications is rather low, as was described by some of the interview partners. Better knowledge of the security certification sector in Austria could have been obtained with a higher response rate from the certification bodies.

3.1.7. References


3.2. **BELGIUM**

3.2.1. **INTRODUCTION**

Belgium has a relatively well established industry for the size of the country.\(^\text{96,97}\) Its location in the center of Europe, makes the country a getaway for trade. It has extensive canal network and very well developed road and rail networks and infrastructure. Antwerp is the largest container port of Europe for US-EU trade. Also the Liege Airport is important center for freight with 339,431 metric tons received only from the U.S. in 2011.\(^\text{98}\) Being the center of the European Union, with most of the services of the EU located in Belgium, large number of people commute to and from Belgium on a daily basis from all over the world. All this activity creates the conditions for the development of a significant security industry, in terms of security of infrastructure and citizens, and the consequent need for security standardisation and certification.

3.2.2. **SHORT DESCRIPTION OF BELGIUM’S SECURITY INDUSTRY**

Belgian industry is active in security and defense, covering a wide area of products and services, from personal equipment to weapon systems.\(^\text{99}\) Also the fields of construction products (steel construction, lifts, heating, storage systems etc.) and mechatronical engineering (machine tools, machinery for agriculture and food industry etc.) are covered. Another sector of Belgian security industry is aerospace, i.e. aeronautics and space (satellites, launchers, navigation). In terms of security of individuals, security measures that are mostly used are those against burglary and hold-ups (81% in 2011), outside surveillance systems (48% in 2011), inside surveillance systems (46% in 2011) and measures against fraud (35 % in 2011).\(^\text{100}\)

The Belgian market for security equipment consists mostly of imported products, apart from safety apparel which is fabricated in the country. Safety and security services from private companies are more popular in Belgium, with more than 800 companies offering services of investigation, surveillance and consultation.\(^\text{101}\)

Quite active in the security field is the Belgian Security and Defense Industry (BSDI), an association with 33 members, created in 1989. It is a group of companies which represents around 90% of the security and defense industry in Belgium. The challenges the Belgian security industry has to confront, as identified by BSDI\(^\text{102}\) are among others, the globalization and delocalization of the industry, the cooperation with multinational stakeholders, the federal and regional division of the country and the shift from defense to security.


\(^{100}\) U.S. Department of Commerce, op. cit., 2013-2014, p. 28

\(^{101}\) U.S. Department of Commerce, op. cit., 2013-2014, p. 29

\(^{102}\) Van De Ven, op. cit., p. 11
3.2.3. **THE SECURITY STANDARDISATION FRAMEWORK**

Belgium has one standardisation body, the Bureau for Standardisation (Bureau voor Normalisatie/ Bureau de Normalisation, NBN). NBN was established in 2003, replacing the former IBN/BIN (Institut Belge de Normalisation). NBN has legal personality and is a public interest body, supervised by the Federal Minister responsible for economy. Until 2003, the Belgian Electrotechnical Committee (BEC/CEB), was also an autonomous standardisation body. With the Standardisation Act of 2003 it continued its standardisation activities, but under the supervision and coordination from NBN. The following figure gives an overview of this document.

<table>
<thead>
<tr>
<th>Legislation</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Art. 4-19 NBN</td>
</tr>
<tr>
<td></td>
<td>Art. 20-30 Superior Standardisation Council</td>
</tr>
<tr>
<td></td>
<td>Art. 31-34 Repealed and amended provisions</td>
</tr>
</tbody>
</table>

Source: Own figure

Figure 8: Overview of Belgian legislation for standardisation activities

According to Figure 9, Belgium has a decentralized standardisation system, as some other European countries. NBN has delegated its standardisation work to sector operators. The sector operators, which are national federations, are responsible for the administrative and technical monitoring of one or more TCs within a specific field. For example, CEB/CEB is one of the sector operators for electrotechnical standardisation. It is possible that one operator is participating in the standardisation work of more than one fields. CSTC (Centre Scientifique et Technique de la Construction/ Wetenschappelijk en Technisch Centrum voor het Bouwbedrijf) participates in more than one TCs related to construction. The Belgian TCs act as “mirror” committees of the EN and ISO TCs. The sector operators are recognised by the Board of Directors of NBN and they need to fulfill a set of criteria, as required by the Standardisation Act.

The different sector operators focus on several security standardisation activities such as personal identification and electronic signatures, maritime and port security services, societal and citizen security and alarm systems. With regard to the TCs of the European and the International Standardisation Organisations, the sector operators participate in the TCs on behalf of NBN. As it is shown in Figure 10. Belgian standardisation is represented in most of the European and International TCs related to security.

---

103 Standardization Act of 3 April 2003, Moniteur Belge/Belgisch Staatsblad 27.05.2003, amended by the Act of 28 February 2013 introducing the code on Economic law.


105 CSTC & SPF Economie, “Normes belges et européennes, Spécifications Techniques Unifiées (STS), Notes d’Information Technique (NIT): Pour une plus grande Qualité des produits de construction et des ouvrages”, p. 7
Figure 9: Representation of the decentralized standardisation system in Belgium

<table>
<thead>
<tr>
<th>European security TC</th>
<th>Sector Operator</th>
<th>International security TC</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEN/TC 224</td>
<td>AGORIA ICT TIC</td>
<td>ISO/IEC JTC 1/SC 27</td>
</tr>
<tr>
<td>CEN/TC 278</td>
<td></td>
<td>ISO/IEC JTC 1/SC 17</td>
</tr>
<tr>
<td>CEN/TC 72</td>
<td>AGORIA – SIRRI S</td>
<td>ISO/TC 21/SC 3</td>
</tr>
<tr>
<td>CEN/TC 114</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEN/TC 127</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEN/TC 143</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEN/TC 147</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEN/TC 391</td>
<td>ANPI</td>
<td></td>
</tr>
<tr>
<td>CEN/TC 325</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEN/TC 263</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEN/TC 370</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEN/TC 52</td>
<td>NBN</td>
<td>ISO/TC 223</td>
</tr>
<tr>
<td>CEN/TC 417</td>
<td></td>
<td>ISO/TC 284</td>
</tr>
<tr>
<td>CEN/TC 419</td>
<td></td>
<td>ISO/TC 272</td>
</tr>
<tr>
<td>CLC/TC 79</td>
<td>BEC-CEB</td>
<td>IEC/TC 79</td>
</tr>
<tr>
<td>CLC/TC 61</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLC/SR 79</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLC/SR 89</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLC/SR 116</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEN/TC 388</td>
<td>SECO-WTCB</td>
<td></td>
</tr>
<tr>
<td>CEN/TLC/TC 4</td>
<td>TSA</td>
<td></td>
</tr>
</tbody>
</table>

Sources: NBN106, 107
Figure 10: European and international TCs on security and relevant sector operators in Belgium

107 For CEN/TC 379 there is no national mirror committee, for CEN/TC 384 no information is provided from NBN
Belgian standards are voluntary, unless they are explicitly referenced as mandatory in a technical regulation as such (law or royal decree). In the fields related to security, NBN has not developed a wide range of security standards additional or replacing the European Standards. The national standardisation activity in the field is limited: according to Figure 11, the NBN standards mainly date back from the 1970’s and 1980’s, with a few exceptions in the 1990’s and 2000’s. They are standards that after their publication were referenced in royal decrees. These NBN standards are still active. They mainly address security issues in households and individuals. In the field of public and semi-public venues, the standards mainly deal with public lighting, fire protection in schools, whereas in the emergency preparedness there are active standards on rescue and firefighting material.

For example, the NBN S 21-205: 1992 sets the requirements for fire protection in buildings and similar establishments and applies to new buildings and extensions to existing buildings in which: a) hotel establishments; b) youth hostels; c) centers for social tourism; d) holiday camps and sports training centers and; e) any other hotel establishments offering accommodation are located. The earlier NBN S 21-204: 1982 addresses the same issue of fire protection but for school buildings, while the NBN 713-020/A3: 1994, also related to fire-fighting covers the fire performance of building materials and products and the fire resistance of building materials.

<table>
<thead>
<tr>
<th>Security domains</th>
<th>NBN Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Border management</td>
<td>-</td>
</tr>
</tbody>
</table>

Source: Own figure\(^{108}\)
Figure 11: NBN homegrown security standards

Additionally to the standards, there are prescriptive normative documents called Technical Prescriptions (Prescriptions Techniques/Technische Voorschriften). The PTVs are established and published by qualified technical institutes, for example PROBETON. PTVs add to an existing standard or fill the gap of the lack of a standard in order to deliver the national mark BENOR to products.\(^ {109,110}\) They are updated regularly to remain relevant and follow the tech-


\(^{109}\) PRC, “Screening national building regulations, Belgium”, 15\(^{th}\) February 2011
ological developments. In the field of road construction and in road restraint systems, vertical signs and road marking, the PTVs are used as a reference document in the regional type specifications and can be used as requirement document for voluntary certification.

Apart from standards and technical prescriptions, Belgium has other normative documents produced by the standardisation bodies, certification bodies or the authorities. These are the following:

- Unified Technical Specifications (STS) (Spécifications techniques unifiées – Eengemaakte Technische Specificaties) are published by the DG Quality and Security of Ministry of Economy. STSs concern the construction sector and describe both regulatory requirements and elements that are not regulated, which are however crucial for the employability and sustainability of the structures. STSs are the result of extensive studies, in which the relevant standards are correlated. They are available to different actors such as the architect, the contractor responsible for carrying out the work, but also the authorities during the procurement process. With regard to the procedure of their development, the Ministry of Economy leads the development and has the general overview of the work. The documents are developed by diverse expert groups with representatives from the authorities, consulting firms and representatives from the industry. STSs are generally voluntary, unless they are referenced in the contractual agreement of the parties and become an obligation, with which a party has to comply.

- Technical Information Notes (Notes d’ Information Techniques/ Technische Voorlicthingsnota’s) have the same purpose as STSs: to help professionals in the construction sector to solve problems they face in terms of understanding and control of all applicable regulatory and voluntary technical specifications and justify their choices, when it is required, to the competent authorities. They provide recommendations in terms of choice of materials and systems for construction and guidance for the implementation of the requirements set by regulations or contractual documents.

- Technical Approvals (Agrément Technique/ Technische Goedkeuringen). Developed by the Belgian Union for technical approval in construction (Belgische Unie voor de technische goedkeuring in de bouw, BUtg). The national technical approvals (ATG) are voluntary assessments, covering both regulated and other characteristics.

---

111 See section below “Selected Security certification bodies and their work”
112 For road restraint systems: PTV869 (steel guard rails) & PTV 124 (precast concrete barriers), vertical signs: PTV662 and road marking: PTV881, PTV882, PTV883, PTV884 and PTV885
114 For Wallonie they are available at Quality and Constructions: http://qc.spw.wallonie.be/fr/index.jsp and Flaanderen at http://qc.aoso.vlaanderen.be/nl
116 The alternative name of the Union in the French language is “Union belge pour l'Agrément technique de la construction” (UBatc)
demonstrating the appropriateness for the intended use.\textsuperscript{116} As a rule, national technical approvals require certification according to ISO system 5, performed by certification bodies assigned by the BUtgb.\textsuperscript{117}

The gap from the lack of standardisation activity in the field of security is filled by the European and International standards. NBN mostly implements standards from the European Standardisation Organisations (EN standards). EN standards are implemented as national NBN EN standards, as provided in the CEN Guide 20 on membership criteria for CEN and CENELEC.\textsuperscript{118}

### 3.2.4. THE SECURITY CONFORMITY ASSESSMENT FRAMEWORK

Based on Belgian legislation summarized in Figure 12, the national accreditation body of Belgium for conformity assessment is BELAC (see Figure 13 for an overview of its characteristics). Since 31\textsuperscript{st} January 2006, BELAC is the only accreditation body in Belgium.\textsuperscript{119,120} The body as it exists today comes from a merger of three bodies: calibration laboratories (BKO), testing laboratories and inspection bodies (BELTEST) and certification bodies (BELCERT). It is under the responsibility of the FPS Economy, S.M.E.s, Self-employed and Energy. Accreditation certificates issued from BELAC are recognised by the Belgian state. BELAC operates on the basis of the Regulation EC 765/2008.\textsuperscript{121}

According to the Quality manual of BELAC,\textsuperscript{122} in practice, the activities of BELAC cover the activities of the following types of bodies: calibration laboratories; testing laboratories; medical laboratories including the activities of Point of Care Testing; inspection bodies; certification bodies for management systems; certification bodies for products; certification bodies for personnel; proficiency testing organisers; producers of reference materials greenhouse gas validation and verification bodies. Figure 14 illustrates this relationship. As the only accreditation body in Belgium, the certification bodies with activity in the field of security certification of PSS (see Figure 15 for an overview) are covered by BELAC.

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{116} UBAtc, Home, no date. http://www.ubatc.be/?lang=en
\item \textsuperscript{118} According to section 5.1., it is an essential duty of the CEN and CENELEC member to implement the EN standard, i.e. to give the ENs the status of national standards and withdraw any conflicting standards: CEN/CENELEC, “Guide 20 on membership criteria of CEN and CENELEC”, 3\textsuperscript{rd} edition, July 2013, p. 26
\item \textsuperscript{119} Loi du 20 juillet 1990 concernant l’accréditation des organismes d’évaluation de la conformité, modifiée par la loi-programme du 9 juillet 2004/ Wet van 20 juli 1990 betreffende de accreditatie van instellingen voor de conformiteitsbeoordeling, gewijzigd door de programmatuur van 9 juli 2004.
\item \textsuperscript{120} Arrêté royal du 31 janvier 2006 portant création du système BELAC d’accréditation des organismes d'évaluation de la conformité, Moniteur Belge, 23 Fevrier 2006
\item \textsuperscript{122} FPS Economy, S.M.E.s, Self-employed and Energy General Direction Quality and Safety, BELAC Secretariat, “Quality manual of BELAC”, p. 16
\end{itemize}
\end{footnotesize}
D2.2: Consolidated report on security standards and certification

CRISP project

<table>
<thead>
<tr>
<th>Legislation</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law of 20 July 1990 concerning the accreditation of the organisations and the evaluation of the conformity [as amended]</td>
<td>Art. 1 Definitions</td>
</tr>
<tr>
<td></td>
<td>Art. 2 National Accreditation Council</td>
</tr>
<tr>
<td></td>
<td>Art. 3 Accredited bodies</td>
</tr>
<tr>
<td></td>
<td>Art. 5,6 Funding responsibility of Service Federal Public Economy, SMEs, Self &amp; Energy</td>
</tr>
<tr>
<td></td>
<td>Art. 7-9 Criminal provisions</td>
</tr>
<tr>
<td>Royal Decree of 31 January 2006 establishing the BELAC accreditation system of conformity assessment bodies</td>
<td>Art. 1 Definitions</td>
</tr>
<tr>
<td></td>
<td>Art. 2 BELAC system</td>
</tr>
<tr>
<td></td>
<td>Art. 3 Criteria for accreditation</td>
</tr>
<tr>
<td></td>
<td>Art. 4,5,6 BELAC organs: Coordination Commission, Accreditation agencies (Bureaux d’accréditation), Secretariat</td>
</tr>
<tr>
<td></td>
<td>Art. 7-11 Procedures for granting, extending etc. accreditation, appeals and complaints funding</td>
</tr>
</tbody>
</table>

Source: Own figure
Figure 12: Overview of Belgian legislation for accreditation

<table>
<thead>
<tr>
<th>Accreditation body</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>BELAC</td>
<td>• Established in 2006</td>
</tr>
<tr>
<td></td>
<td>• Responsibility of FPS Economy, S.M.E.s, Self-employed and Energy</td>
</tr>
<tr>
<td></td>
<td>• On the basis of EC 765/2008 Regulation</td>
</tr>
<tr>
<td></td>
<td>• Issues certificates recognised by the Belgian state</td>
</tr>
</tbody>
</table>

Source: Own figure
Figure 13: Belgian accreditation body and characteristics

The evaluation of conformity assessment is based on the international standards for accreditation, such as the standard NBN EN ISO/IEC 17020 for inspection bodies and the standard NBN EN 45011 or Guide ISO/IEC 65 for products certification bodies.

BELAC is a signatory of all existing MLAs (multilateral agreements) and MRAs (multilateral recognition agreements) of EA, ILAC (International Laboratory Accreditation Cooperation) and IAF (International Accreditation Forum).125

125 FPS Economy, SMEs, Self-employed and Energy, Conformity of products and services a tool to boost confidence: accreditation of laboratories, inspection and certification bodies, http://economie.fgov.be/nl/modules/publications/general/belac_folder_fr_conformite_des_produits_et_des_services.jsp
Chapter 3.2.5 describes the work of these organisations in more detail.

### 3.2.5. SELECTED SECURITY CERTIFICATION BODIES AND THEIR WORK

As mentioned above, in Belgium there are among others certification bodies for quality systems, environmental management, products certification bodies and persons certification bodies, accredited by BELAC. These bodies, as it will be further elaborated below, issue certificates based on standards and other normative documents.

#### 3.2.5.1. CERTIFICATION SCHEMES

In Belgium, there are regulatory and voluntary certification schemes, which are national, pan-European or international. Example of the pan-European voluntary ones are:
• The voluntary ENEC (European Norms Electrical Certification)\textsuperscript{126} for safety of electrical products in compliance with ENs and
• The voluntary HAR mark for cables and cords complying with Harmonized specifications,\textsuperscript{127} certified by SGS.

At national level, INCERT certification for intrusion detection and related security areas is offered by several bodies and quite popular.\textsuperscript{128} More specifically, INCERT is a national quality mark for security installations against intrusion, in particular for products and services of electronic security against intrusion in buildings.\textsuperscript{129} Security companies bear the INCERT mark, when compliant with the "Regulation of Corporate Safety Certification" and the realization of the facility in accordance with "General requirements for alarm systems T 015/2 intrusion" published by the Belgian Electrotechnical Committee CEB. For products, the permission to bear the brand INCERT is a result of a certification of their compliance with the "General requirements for the testing of alarm systems T014 or T014A" published by the CEB. The following figure gives an example for the INCERT certification framework.

![INCERT Certification Framework](figure16.png)

Source: Own figure
Figure 16: Example of the INCERT certification framework for remote surveillance centers

### 3.2.5.2. SELECTED CERTIFICATION BODIES

**ANPI**

ANPI (National Organisation for fire and theft protection formerly National Fire and Intrusion Protection Association) is a non-profit organisation active in the field of standardisation as one of the sector-operators of NBN.\textsuperscript{130} Apart from the standardisation activity, ANPI has other divisions such as certification, inspection, information and laboratories.\textsuperscript{131} In terms of security certification, ANPI certifies among others products for anti-theft mobile objects

\textsuperscript{127} EEPCA, About the HAR Mark, no date. http://www.eepca.eu/page.php?p=192
\textsuperscript{129} INCERT, Secteurs d’activité, no date. http://www.incert.be/fr/secteurs.html
\textsuperscript{130} ANPI in the context of its activity as sector operator participates in the following TCs: CEN TC 79, CEB TC 79, CEB PCP 79, PCP 301, TC 263, TC 391, TC 405.
\textsuperscript{131} ANPI, Who is ANPI?, no date. http://www.anpi.be/launch.cfm
(alarm systems, remote immobilization systems, tracing systems, speed reducing and ignition prevention systems), security companies for installations in buildings (installers of alarm detection systems), products for protection of buildings (detectors, warning devices, control and indicating equipment, systems with voice communications using the PSTN tec.), remote surveillance centers, safes, locksmiths and façade elements. In the area of fire and theft prevention certification, ANPI certifies based on the following schemes: Certalarm,\textsuperscript{132} INCERT,\textsuperscript{133} I3 for façade, S3 for locksmiths,\textsuperscript{134} BOSEC, BENOR and others. The organisation also has its own certification scheme for theft and fire prevention certification. With regard to the documents that form a basis for the testing and certification processes, ANPI uses standards, legislation and other documents such as ANPI internal rules and the rules of the several certification schemes:\textsuperscript{135}

\textsuperscript{132} CERTALARM, Home, no date. http://www.certalarm.org/ca/
\textsuperscript{133} See previous section
\textsuperscript{134} Read further ANPI website http://www.anpi.be/index.cfm?ee=2|749
Standards | Legislation | Other documents
---|---|---
Low Voltage Directive[^137]

Source: Own figure[^138]
Figure 17: Documents for ANPI certification activities

For the certifications that ANPI issues, the minimum evaluation criteria are Certalarm scheme rules[^139], INCERT scheme rules[^140], ANPI scheme rules[^141], I3 scheme rules[^142] and S3 scheme rules[^143]. The following figure provides an overview of their quality seals.

![ANPI quality seals](source)

Source: Own figure[^144]
Figure 18: ANPI quality seals


[^139]: Certalarm, Home, no date. [www.certalarm.org](http://www.certalarm.org)

[^140]: INCERT, Home, no date. [www.incert.be](http://www.incert.be)

[^141]: ANPI, Home, no date. [www.anpi.be](http://www.anpi.be)

[^142]: ANPI, op. cit., no date.

[^143]: ANPI, op. cit., no date.

[^144]: Information from ANPI
Vinçotte

Vinçotte was established in 1872 and has today a share of around 75% of the Belgian market.\textsuperscript{145} It has 16 establishments worldwide and around 15,000 industrial customers.\textsuperscript{146} Its activities spread in more than 130 services (electricity, hoisting apparatus, pressure equipment, civil engineering, safety in the work place, environmental protection and radiant protection) in a variety of sectors.

In the sector of PSS certification, Vinçotte provides certification services, such as the voluntary INCERT certification for security companies, the harmonised EN 1090 series (Eurocode) for steel or aluminium construction, the Achilles prevention system and others.

With regard to the process of certification of a voluntary scheme, we take as an example the case of INCERT. According to Vinçotte, the certification process of INCERT is as follows:\textsuperscript{147}

- Initial evaluation of the application file submitted by the security company, in particular a. the validity of the approval issues by the Federal Public Service of the Interior is verified b. the professional experience, the organisation chart and the list of employees, and subcontractors, etc. is examined c. the insurance policies taken out as well as other financial and fiscal conditions are reviewed.
- Initial evaluation of the conformity of the activities of the security company with the normative documents, among other through: 1. Administrative audit and b. technical evaluation of the work (installations) concluded by the company.
- Follow-up administrative audits of the company (2 audits within 5 years), verification of probative documents
- Technical evaluation of installations done by the company every year.

BCCA

BCCA is the Belgian Construction Certification Association. It was established in 1992 by the Technical Bureau Control for Construction (SECO) and the Belgian Building Research Institute (BBRI) with the aim to create a system in the area of certification. BCCA is a specialised certification body in the construction sector for products and construction systems, organisation systems, management systems, persons and processes. BCCA is active in all types of certification procedures - legal procedures via governmental decree as well as voluntary procedures based on consensus between parties.\textsuperscript{148}


The area of certification of products, product systems and construction systems is a substantial part of the work of BCCA in terms of volume. It includes initial technical assessment of

the products and systems as well as following up the quality of production and labeling. A distinction can also be made between certification aimed at conformity of the products and certification which only assesses the production control system (FPC). With regard to the certificates, BCCA issues national level certificates such as the BENOR certificate for compliance with Belgian standard or normative specification, ATG certification in addition to Technical Approvals granted by the Belgian Union for Technical Approval in Construction (BUtgb), as well as pan-European ones such as the CE symbol and the CEN Keymark.

Interesting in terms of security and safety is the VCA certificate, a programme whereby service-supplying companies may be tested in a structured and objective manner, and certified for their VCA administration system. VCA stands for (in Dutch) Safety, Health and Environment Checklist for Contractors and among others the activities that are certified are mechanical engineering activities (maintenance work, construction) electro-technical activities and process control (maintenance of electrical systems) and other technical services such as fire and manhole guards, security guards etc. The scheme often offers a concrete and practical implementation of statutory schemes or supplements them. For instance, a contractor with SCC certification demonstrably complies with a number of obligations laid down in the national legislation on labor conditions. The certificate originates from the Netherlands, but since 1999 is also operational in Belgium managed by the association BeSaCC (Belgian Safety Criteria for Contractors). Moreover, it is recognised in other countries such as Germany.

3.2.6. SUMMARY AND CONCLUSION

Belgium is a small European country with a rich railway and road network, as well as airports and harbours, such as the Antwerp cargo, which comprise the critical infrastructure of Belgium. The country has also a significant security industry, especially as it relates to the security and defence field and the provision of security services.

The decentralized standardisation system in Belgium allows for the combination of participation of experts from varying fields of knowledge, referred to as national federations, with centralized oversight by the NBN, making it one of the strongest good practices identified in Belgium. The national federations, under the supervision of the NBN, are responsible for the development of “home-grown” standards and the Belgian contributions to European and International standardisation efforts.

Unified technical specifications (STS) support manufacturers by providing a singular normative document (e.g. technical prescriptions, technical information notes, etc.) for varying fields specifying the requirements that must be met, effectively mitigating fragmentation in the field of standardisation.

---

153 For more information, see the website of BeSaCC: http://www.besacc-vca.be/fr/content/info-besacc
154 VCA, Frequently asked questions, “How international is the SCC?” http://english.vca.nl/frequently-asked-questions/scc.aspx?faiId=45#45
Also positive is the use of national level quality marks, trusted by the demand side of the Belgian market and the public. On the other hand, the use of national quality marks is of territorially limited recognition.

Accreditation in Belgium is the responsibility of the accreditation body BELAC, which operates under the responsibility of SPF Economy, S.M.E.s, Self-employed and Energy. BELAC accredits a wide range of bodies, including certification bodies for products, services and personnel.

Security certification bodies base their certification activities on standards and the other types of normative document. Many of the certification bodies, e.g. BENOR, ANPI, Vincotte and BCCA, maintain their own label of quality, but opt also to use regulatory or voluntary certification schemes. BENOR, BCCA and ANPI are well-established quality marks for the construction sector. Vincotte offers security certificates in the fields of fire and theft alarms as well as information security. Each are notified bodies that issue certificates on pan-European and Belgian standards, as well as technical specifications and marks.

3.2.7. REFERENCES

Arrêté ministériel du 14/01/1999 interdisant la mise sur le marché de différents appareils électriques déjà interdits dans un autre pays de l’Union européenne - Ministerieel besluit houdende verbod de verschillende elektrische apparaten die reeds in een andere Lidstaat van de Europese Unie zijn verboden in de handel te brengen, Moniteur belge.

Arrêté royal du 23/03/1977 déterminant les garanties de sécurité que doivent présenter certaines machines, appareils et canalisations électriques - Koninklijk besluit tot vaststelling van de veiligheidswaarborgen welke bepaalde elektrische machines, apparaten en leidingen moeten bieden, Moniteur belge du 31/03/1977 Page 4086.


Member States relating to electrical equipment designed for use within certain voltage limits (codified version) was published in the OJEU L 374 of 27.12.2006


FPS Economy, S.M.E.s, Self-employed and Energy General Direction Quality and Safety, BELAC Secretariat, “Quality manual of BELAC”


3.3. FRANCE

3.3.1. INTRODUCTION

With a geographical size of 632,833.6 km² and a population of 65.9 mn (2014) France is the largest EU country from a geographic point of view and the third largest country regarding its inhabitants. The most important sectors of France’s economy are public administration, defence, education, human health and social work activities (22.6%), wholesale and retail trade, transport, accommodation and food services (18.3%) and real estate activities (13.2%). France has also a strong security industry and the incidents in Paris in January 2015 highlight the importance of security measures in a specific way. This chapter presents the country’s security standards and certification system.

This France country study will analyse the general characteristics of the French security system. In this regard, not only the mechanisms, structures, strategies and the current state of the security system are investigated, but also the cultural, economic and administrative foundations of the French political system and its historic condition. After a sketch of the general country system this country study will attempt to identify the individual characteristics and principles of the French security system with regard to security standardisation framework, the conformity assessment framework and the security certification. As a working basis, literature sources, legal texts, monographs, articles, job reports and expert interviews were used.

3.3.2. SHORT DESCRIPTION OF THE COUNTRY’S SECURITY INDUSTRY

3.3.2.1. THE ADMINISTRATIVE STRUCTURE OF FRANCE

Initiated by the French Revolution and Napoleon, France was coined almost two centuries by a pyramidal, strictly centralized character. Today, the political-administrative structure of France, despite decentralized efforts, is still characterised by a power imbalance in favor of centralism. This claim of power is especially enforced and protected by the Parisian (central) authorities as well as by the downstream prefectural system. In Paris all important decision-making processes converge and the decision-making powers of local authorities is in most cases very limited.

The political structure of France is basically characterised by two groups of public actors: the central government on the one and three local authorities on the other side. Expressed in figures, these include 22 regions, 96 departments, 36,564 communes. These three types of local authorities coexist in France and there is no principle of subsidiarity, as a region. The result is a complex juxtaposition of local authorities and other institutions that in consequence often overlap in the areas of competence. The Parisian ministries practice in addition to traditional jurisdictional responsibilities (economic, defense, home affairs), other tasks (spatial planning, agriculture, culture).

156 European Union, op. cit., 2015.
In France (as of 2012) there are 36,564 municipalities. Thus, France has compared to the Germany for example (16,061) twice as many communities, although three of four French citizen living in urban areas. 21,000 French municipalities have less than 500 inhabitants, which means these communities are usually very small. Due to the extremely small population, the communities usually lack of financial and human resources to get involved politically. Special-purpose associations and cooperation in community management often alleviate the lack of resources.\(^{159}\) This broad distribution of many small communities challenges the French security and protection system to change to a nationwide uniform level and to set common security standards.

### 3.3.2.2. The French Security Market

Since the market for security is very wide and diverse it can be classified in four different categories of enterprises. In general there are two main characteristics for security enterprises: How international it is? How standardised are the products or services? From those two main characteristics the security market can be derived the four categories:\(^{160}\)

- **Category 1:** International and standardised products/services. Those companies are usually companies dealing with video surveillance or larger security infrastructures or again in human surveillance services.
- **Category 2:** International and products/services adapted to each client. Those are usually companies which offer technical or advisory services linked to either a particular situation or risk which therefore require flexibility and adaptation to each client’s particular case. As an example he names anti-corruption programmes and fighting against inside fraud.
- **Category 3:** National and standardised products/services. Those companies are actually often institutions responsible for the formation of security agents. Else they are the ones covering the domain of electronic security and surveillance in accordance to the French specific laws.
- **Category 4:** National and products/services adapted to each client: As in the case with the international companies, these national companies are more oriented towards advisory services. They for example advise the top management of other enterprises in crisis situations. A crisis being never the same, they adapt their service to the situation and client.

The French security sector has been steadily growing in the recent years. There are several possible reasons for such a development: 1. Insurance companies are putting more and more financial pressure on their clients to get better and higher security if they wished to keep their insurance. 2. The growing fear of terrorism, especially with companies abroad; 3. The steadily expanding French companies, which now are (due to the internationalization) stationed abroad and face different threats than on French soil and which are no longer protected by the French government; and 4. The growing market share of foreign security companies (in 1990 the market was composed of 20% foreign firms compared to in 2007 where it is 40%).\(^{161}\)

---


\(^{161}\) Schild, Joachim, and Henrik Uterwedde, op. cit., 2006.
Usually the bigger the security companies the more services they offer and are no longer specialized in one or two domains (and may even belong to more than one category from above). The trend is currently towards diversification of strategies which strengthens the bigger companies. Positive effects of this tendency is that there is a growing demand for regulations, norms and quality certifications. The reasons behind this wish are that the larger companies hope to eliminate the competition and create barriers to market entry\textsuperscript{162} but they are still useful for society. Especially with the recent market explosion where a lot of companies offered services of dubious quality for dumping prices and undermined companies of higher qualities but also prices.\textsuperscript{163}

With the help and influence of the USP “l’Union de Sécurité Privée” (so the union of the private security) was passed a modification of a law, namely the “Décret n°2007-1181” which modified the law from 1983 which regulates the activities of the private sector of security and other domains.\textsuperscript{164} The new Décret demands that managers and employees operating in any of the fields named in the law of 1983 (so private security, CIT, human surveillance, bodyguards of all types) must be able to prove their competency through the ownership of either of the following documents:

- A Professional certification (also named trade certification) for the named above activities or
- A qualifying certificate developed by the domain and acknowledged by the ministry or
- A title, recognised inside of the European economic market or by any Member States.\textsuperscript{165}

Data of the French market for security services are provided by CoESS\textsuperscript{166}. According to the source, the turnover was € 5.29 bn in 2010 including General guarding (excluding the segments listed hereafter): € 3.67 bn, Airport security: € 365 million, Cash-In-Transit (CIT): € 5 million, Monitoring and remote surveillance: ± € 590 million. Other relevant segments include in particular: Bodyguarding: € 50 million and Security training: € 40 million. Unfortunately, the source does not provide information on technical services such as planning, installing etc.

From a report\textsuperscript{167} by the U.S. Department of Commerce (U.S. Commercial Service) the following information on the market in general can be obtained. According to the report, French Safety and Security industry is represented by 22 segments. At this, the market is very fragmented and competitive. In 2011 the market had a total value of approximately € 20.8 bn (latest official public figure available at publication of the report). Growth rates of the industry

\begin{itemize}
  \item\textsuperscript{162} E.g. compliance to certain regulations employs a first investment to enter a particular market segment.
  \item\textsuperscript{165} Schild, Joachim, and Henrik Uterwedde, op. cit., 2006.
\end{itemize}
D2.2: Consolidated report on security standards and certification

CRISP project

differ by segment but are, closely linked with the development of the French economy, relatively low (4% in 2011). 16 out of the 22 segments had a growth rate of more than +1%. The segment with the highest growth rate was IT security (+17.1%), whereas guarding showed the biggest decline (-1.7%). In 2011, 63.4% of the companies active in safety and security industry were turning profit, 10.3% left the market. This goes at hand with a process towards a more selective environment and a maturing of the sector. Also, an ongoing concentration of market power can be observed, in 2011 the top 5 players held 29.8% of market shares.

The European Commission is aware of the lack of updated data including comparable data at all Member States and entrusted ECORYS with a market study of key European countries, which will also include France. The study will be completed in summer 2015. According to preliminary data, the turnover of the French security industry is € 20.4 bn, which is accomplished with 215,000 employees (see country study ‘Poland’).

3.3.3. The Security Standardisation Framework

3.3.3.1. The French Security System

One of the main tasks of modern states is to protect its citizens against specific hazards which cannot be fended alone. On January 7, 1959, the concept of “Total Defence” of the French nation (“global defense”) was decided.\(^\text{168}\) The main objective of the overall defense of the French population is that it is no longer the sole responsibility of the military forces, but also the responsibility of the economic and civil defense system to protect its citizens. The latter include the areas of logistics, civil protection and the maintenance of everyday life. In this regard, the French defense systems affects all basic institutions of the state.\(^\text{169}\)

At least since 2004, the term that characterises the French public or civil security is ‘sécurité civile’. The aim of sécurité civile is to protect people, the environment and aims at risk prevention. Although defined by international law and applied in some neighboring European countries (e.g. Belgium), the concept of civil defense (“protection civile”) is considered outdated and not comprehensive enough. Due to the centralism, the French security system is uniformly organised and standardised by law. Competencies are distributed on several levels which can be differentiated as Nations, Zones, Circles, Communities as well as inter-municipal levels. These territorial levels are subject to different chains of command to inform respective authorities and professional services and carry out the exercise of the tasks assigned to them. At the ministerial level, the security of civil defense has to endure a broad political fragmentation in the Ministries of Interior, Health and Agriculture. The ministry of the interior is responsible for civil defense, the maintenance of public order, security of people and critical infrastructure. Even though France is a centralistic state the issue of security was organised cross departments. Because of this fragmented political responsibility in matters of defense or security, individual ministries such as the Department of Civil Defence & Security (“Secrétariat General de la Défense Nationale) have an important coordinating function.

---


3.3.3.2. SECURITY STANDARDISATION AT AFNOR

AFNOR (Association Française de Normalisation) is the French national organisation for standardisation. AFNOR and bodies appointed to AFNOR ensure the issuing of standards and the promotion of such standards in France and on the international level. The standardisation principle relies on consensus driven decision making ensuring the openness to all interested parties. On the international level AFNOR represents the French perspective on national standardisation and translates international documents to the French language (e.g. ISO, ETSI, IEC). Furthermore AFNOR is organising the national public consultations on international documents. AFNOR certifies the final version of translated documents and integrates the standards documents in the national catalogue. In France, homegrown standards are usually drafted by the particular sector based standardisation office (BNS). For broad topics or topics that have importance across industries, AFNOR is drafting standards without the BNS approvals. AFNOR is responsible for ensuring interoperability among standards and the coordination of different standardisation projects. In this regard the French standardisation system is structured in several large standardisation programmes, coordinated by the French Standardization Coordination and Steering Committee (CCPN). The large programmes are set to search for new areas for standardisation. The appointed Strategy Committee (CoS) identifies the standardisation needs, while AFNOR ensures conformity to needs on the national, European and international level.

AFNOR is associated to several key network partners. The network partners are developing standards and specifications that are accredited by AFNOR. Technical expertise is thus allocated among third organisations to ensure technical expertise for specific topics of technology. Partners in e.g. information provision, standard setting, certification and training are: ADEME (French Agency for Environment and Energy Management), ADEPT (Association for the development of international trade in food products and techniques), COFRAC (French Accreditation Committee), CSTB (Scientific and Technical Center for Construction), CTI (Center Network industrial technology), INERIS (National Institute for Industrial Environment and Risks) emerged from CERCHAR (Study and research centre of the Charbonnages de France), LNE (Laboratoire National Metrology and Testing) such as UTAC (Union Technique de l'automobile, cycle and motorcycle).

AFNOR- security and safety standards

While the French society is in a constant changed influence by a rapid change of technology and life-style, also security and safety issues increasingly changed during the last decades. In this regard, the need for security is not limited to physical security but also extents to a so called moral security (refusing, even indirectly, to be involved in any kind of violation of people's fundamental rights). AFNOR has created a safety and security group with the goal to recognise and integrate these security trends. In this regard anticipating security problems of the future is important to set a standard right in place. In the AFNOR security group most topics concern health and hygiene, the precautionary principle and personal safety. Figure 19 displays all security issues that are part of the security standardisation framework.

---

170 Moral security refers to health and hygiene, the precautionary principle and personal safety.

### Security Topics

<table>
<thead>
<tr>
<th>Accident and disaster control</th>
<th>Occupational safety. Industrial hygiene</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm and warning systems</td>
<td>Protection against crime</td>
</tr>
<tr>
<td>Character sets and information coding</td>
<td>Protection against dangerous goods</td>
</tr>
<tr>
<td>Company organisation and management in general</td>
<td>Protection against electric shock. Live working</td>
</tr>
<tr>
<td>Crash protection and restraint systems</td>
<td>Protection against excessive pressure</td>
</tr>
<tr>
<td>Domestic electrical appliances in general</td>
<td>Protection against fire</td>
</tr>
<tr>
<td>Domestic safety</td>
<td>Protective equipment</td>
</tr>
<tr>
<td>Electrical apparatus for explosive atmospheres</td>
<td>Radiation protection</td>
</tr>
<tr>
<td>Electrical engineering in general</td>
<td>Safety of machinery</td>
</tr>
<tr>
<td>Explosion protection</td>
<td>Seismic and vibration protection</td>
</tr>
<tr>
<td>Nuclear power plants. Safety</td>
<td></td>
</tr>
</tbody>
</table>

![Table](https://via.placeholder.com/150)

**Figure 19:** Security standards topics in France

### AFNOR/SECU Security and protection of citizen

The AFNOR/SECU committee is responsible for social security and protection of civilians to set organisational standards (process standards) on the one hand and technological (technical solutions) standards on the other hand. In this regard AFNOR/SECU is responsible for different application areas. AFNOR/SECU is developing safety standards to monitor, prevent or predict disaster situations, reduce or eliminate the consequences of disasters, put in place the tools and civil protection equipment, training and education populations and the provisions that allow the continuity of economic activities in times of crisis. The aspects covered by the "Security and Citizen Protection" are: citizen protection, the protection of infrastructure and networks, protecting vital points, network protection, border protection, protection of transport (air, land and sea), planning and crisis management, the definition of public-private partnerships, coordination and cooperation of relief, the emergency preparedness / business continuity & resiliency, security of information systems (SSI), the response to a threat of nuclear nature radiological, biological, chemical and explosive and video surveillance.

### The French standard setting activities for citizen protection

France has been an important player in the development of the ISO/TC 223. At the invitation of AFNOR, the ISO/TC 223 group met in May 2009 in Saint-Denis at the headquarters of AFNOR. Beyond the mere interest in the subject of social security, the French delegation showed its real commitment to the TC. Its missions address extremely broad issues to help to ensure the safety of the citizen, so that they can live free, in peace and away from danger in an environment that is not harmful to people’s health or wellbeing.

Some 120 international delegates from AFNOR contributed to the progress of several projects of standardisation of security products and services. Notable among these: command, control and cooperation in the management of emergency situations, including information systems.
for crisis management and warning procedures; Public-private partnerships for prevention and risk and crisis management, the operating continuity (business continuity) in a crisis, societal security management systems, interoperability formats to digital video surveillance. France is distinguished by the strength of its contribution on several topics, including the management of crisis situations, business continuity and video surveillance. The French active membership in the TC has shown the extent of the French investment in security standardisation. Figure 20 displays the standards issued by TC 223.

At AFNOR, the "Security Forum" is co-chaired by a manufacturer and a representative of the Ministry of Interior. This platform of exchanges implements actions on the social security sector, forecasts and coordinates normative developments, which makes it extremely rewarding for participants. It is open to all. It is noteworthy that was made official a new European TC (CEN TC 391) "citizen protection" including the forum actively follow developments.172

<table>
<thead>
<tr>
<th>Standards issued by the TC 223 with French contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>- ISO 22300, vocabulary</td>
</tr>
<tr>
<td>- ISO 22301, preparedness and continuity management systems requirements</td>
</tr>
<tr>
<td>- ISO 22311, video surveillance for interoperability</td>
</tr>
<tr>
<td>- ISO 22320, command and control, coordination and cooperation for emergency management requirements</td>
</tr>
<tr>
<td>- ISO 22322, public warning</td>
</tr>
<tr>
<td>- ISO 22397, private and public partnerships</td>
</tr>
<tr>
<td>- ISO 22398, guidelines for exercises and testing</td>
</tr>
<tr>
<td>- ISO 22399, guideline for incident preparedness and operational continuity management</td>
</tr>
</tbody>
</table>

Figure 20: Standards issued by ISO/TC 223 with French contribution

As explained by an interviewed engineer at AFNOR, the following issues relate to societal security: "...social security is everything that helps to protect the civilian population." Norms and standards are regarded as one of the core functions of the state: "...setting standards for safety equipment, such as ensuring that communication between firefighters and gendarmes are interoperable is fundamental to ensure that systems work together "the engineer adds. France has decided to develop security standards to monitor, prevent or predict disaster situations, reduce or eliminate the consequences of disasters, to place civil protection tools and equipment, train and educate people about situations of disasters and implement the provisions that allow the continuation of economic activities in times of crisis. Societal security encompasses business continuity plans (BCP) (see Issues No. 278). "The PCA is one of the pieces of the great puzzle that is societal security," the interviewed engineer said.

At the end of 2013, the ISO published the first reference document ratified internationally dealing with incident preparedness and continuity management for organisations in the public sector and the private sector. The Publicly Available Specification ISO / PAS 22399: Societal

---

security - Guidelines for incident preparedness and operational continuity management is based on the best practices of national standards. The document has been initiated in the framework of a meeting of a workshop in Florence (Italy) in April 2006, which resulted in two days to make a document called "Best of 5 "together the common structural elements and standards of different countries: NFPA 1600 (National Fire Protection Association standard) (see Issues # 275 of Homeland Security), HB 221, BS 25999-1, a Japanese document and another Israeli.

The work was subsequently been transferred to the ISO/TC 223, whose mission was to make the document compatible with ISO 9001, 14001 and 27001. An interviewed Secretary of ISO/TC 223 said: "The guidelines provide a basis for understanding, developing and implementing incident preparedness and operational continuity management within an organisation and to build confidence in relations organisation / community, business / enterprise and organisation / client. They are a tool for public and private organisations to consider the factors and steps necessary to prepare for any incident, whether intentional or natural (interruption, emergency, crisis or disaster) so that they can manage and survive and take appropriate measures to ensure the sustainability of the organisation. The document is a guide for societal security."

The specification represents a major advance in the treatment of preparedness for emergencies and disaster response capacity and continuity. The ISO / PAS 22399 establishes the process, principles and terminology of incident preparedness and business continuity management (business) in the context of social security. The ISO explained in the paper, "Organizational resilience requires proactive preparation for potential outages and incidents in order to avoid the suspension of operations and critical services, or to provide for their recovery as quickly as those who depend on demand. The ISO / PAS 22399 describes a holistic management process that identifies potential impacts that threaten an organisation and provides a framework to reduce their effects to a minimum.” International cooperation in the ISO/TC 223 will increase in coming years to help organisations and communities to address common emergency situations and survive.173

Security standardisation with French involvement

Technical standards dictate, as well as legal standards174 in terms of quality organisational rules for companies (ISO 9000), environmental (ISO 14000), health and safety, food safety (ISO 22000) or safety in transportation. This is the case of the ISO 28000 standard. This standard is a specification for security management systems for the supply chain. It defines the requirements to allow a business to establish, implement and improve a management system for safety, including critical aspects for ensuring the security of the supply chain. These elements relate, without limitation, the aspects relating to finance, manufacturing, information management and packing facilities, storage and transfer of goods between different modes of transport and the various places. In the same context, a "working group" was organised on the protection of drinking water systems. Standards thus deal with the human and political organisation and in particular public safety, and competing with the law provisions. They define, in addition to the technical characteristics of products or services, organisational operational


174 Legal standards refer to regulations
modes. This includes for example the modalities of human control organisation. Thus, one can imagine that the screening of passengers at airports will eventually be entirely defined by international standards. As part of a variation or a takeover of the U.S. programme on defense and security of the citizen, extensive global and European programmes have tackled the production of norms and standards.

A significant number of national and international bodies are working on the standardisation of citizen security. These organisations are in charge of the issues of standardisation and interoperability of equipment, which has just published the ‘Strategic Plan for Developing a suite of Chemical, Biological, Radiological, Nuclear, and Explosives Protective Equipment Standards’. This structure brings together local authorities, regional and federal in the field of health and safety in the event of major accidents. It is particularly known in the chemical sector, Biological, Radiological and Nuclear. Apart from issues of state agencies structures, a majority of working groups were derived from national standards bodies (AFNOR France), European (European Committee for Standardisation - CEN, CENELEC) or international (International Organization for Standardization ISO/IEC) (see Figure 21). These specialized working groups on various topics. We give an extract of the topics to drive, both to show the scope, variety and provide useful information (see Figure 21).

There are probably a thousand worldwide whose work often overlaps. Competition between groups and entities that host is as lively as the cooperation that can exist between them. On the one hand different standard setting groups may have special interests for particular topics of their interest. In these cases groups often compete for the same security issues. In other cases cooperation among groups may accelerate the use and spread of standards created by one group through the promotion of another.

3.3.3.3. THE FRENCH GIS - SECURITY AND CITIZEN PROTECTION GROUP

In January 2004, the Advisory Group "Security" of ISO, was created to coordinate the normative work to strengthening the security of citizens. Meanwhile, seized by the European Commission which saw U.S. initiatives risk of barriers to transatlantic trade or protectionism in disguise, CEN has set up a working group, CEN WG 161 "Security and protection the citizen." The attacks in Madrid and London have increased the awareness of European citizens faced with the terrorist threat. At national level, the Strategy and Outlook Committee (COP) of AFNOR, decided to create a pulse Strategic Group ("Groupe d’Impulsion Stratégique“, GIS) to track all these initiatives and to train the national position on this issue, see Figure 22). GIS brings together the most relevant administrations (Interior, Defense, Industry, etc.), the most active industry in the global security industry (EADS, Thales, Sagem, etc.) as well as users of products and security systems.175

| Civil Defence and Security (ISO/TC 233) | ISDEM (Information System for Disaster and Emergency) (CEN WS) |
| Citizen Security (CEN WG 161) | CAP: Common Alerting Protocol (OASIS) |
| NATO Air Force Armaments Group (NAFAG) | PSCE (Public Safety Communications in Europe) Emergency) (CEN WS) |
| Security Forum (AFNOR) | Alarm response CEN TF |
| Humanitarian Demining (CEN WS 12) | Alarm systems (IEC TC 79) |
| Private security services (AFNOR CN) | Traceability of containers ICSO (International Container Security Organization) |
| Forgery | Intelligent Transportation System (ISO/TC 204) |
| Water security CEN TC 164 | Equipment for the emergency services and control against fire (CEN TC 192) |
| Maritime Transport | Radiation protection (ISO/TC 85 SC 2) |
| Risk Management (ISO TMB WG) | Electronic Citizen Card (ECC) (AFNOR CN) |
| Biometrics (ISO IEC JTC 1 SC 37) | Detection systems and fire alarm (CEN TC 72) |
| Identification Cards and personal (ISO IEC JTC 1 SC 17) | Doors and windows (CEN TC 33) |
| Personal identification and digital signature (CEN TC 224) | Explosive atmospheres (CEN TC 305) |
| Information system risks (IRIS) (AFNOR / X08S) | Fire detection and alarm systems (ISO / TC 21 / SC 3) |
| Technology Security Techniques information (ISO IEC JTC 1 SC 27) | Fire safety (ISO/TC 92) |
| Best practices for the design and development of information systems critical (CEN WS) | Safety devices (AFNOR CN) |
| Emergency Telecommunications (ETSI EMTEL WS) | Hazards to humans and the environment due (ISO / TC 21 / SC 3) |
| Emergency Preparedness | Containers for transport of goods (ISO / TC 21 / SC 3) |
| Emergency Situation (ISO WS) | |

Figure 21: The key groups in security standardisation with French involvement
The mandate of GIS "Security and Citizen Protection" specifies the scope and group assignments. The scope is the security and protection of citizens. Specifically, it focuses on standards that contribute to strengthening the security of individuals against all forms of threats, malicious threats and acts that may affect their daily lives (terrorism, organised crime, crisis, health disasters, epidemics, etc.). The four main objectives of the GIS are:

- Establish a platform for exchange to mobilize and unite the communities affected by the themes of security and protection of citizens in order to promote the exchange of information.
- Follow the different initiatives that develop on the subject in various fora both at European and international level (ANSI, ISO, CEN, ICT Standards Board, etc.).
- Consolidate the French positions, to establish a uniform doctrine whatever levels (national / international, regulatory / normative) and identify priority subjects standardisation based on the added value that can bring standardisation.
- Contribute to CEN and ISO work to identify and name the French experts to defend national positions within strategic groups set up so as to CEN ISO.\textsuperscript{176}

The group was established for several specific reasons. While France was among the initiators of international security standardisation, a problem of France is the lack of presence in the standardisation bodies especially in international meetings. This criticism mainly concerns globally and the 13 French directors and consumer associations. The causes of this failure are numerous.\textsuperscript{177} Participation in countless standardisation work is, as the laws or regulations, a


\textsuperscript{177}\textit{AFNOR, Khémili, A., op. cit., 2006}
heavy human and financial investment. Meetings are often held around the world. The French civil law and the hierarchical organisation badly adapt to a system similar to that of the common law where the rules are derived from a regulatory process that starts from the bottom, through experience, experimentation, grope and debate, and not that starts from the top, the power to impose on all; what is called a process of "bottom-up" process against the "top down". While the legislative process is the result of cross consensus, it undermines our organisational silos between departments. While many are aware of this situation and redouble the French efforts remarkably AFNOR to sensitize national stakeholders, it is clear that the French mobilization and European cohesion are still perfect. ISO established a TC on civil defense entirely in the hands of the Swedes and Americans. The British launched a similar group in Europe (CEN) where France is yet not present. The GIS group was established to overcome this problem.

3.3.3.4. Specific Standardisation Issues

If equal living conditions are sought in Europe, that also means that the citizens of the European Union can expect the same high level care of the security (e.g. in the field of fire protection and emergency medical services). Interoperability is a central aspect on which security will be measured. In order to face new challenges, such as national boundaries, the interoperability of existing systems must be ensured so that the various national security components can engage effectively. With the so-called European Civil Protection Mechanism, a tool has been created to improve cross-border cooperation in civil protection more efficiently. However, these cross-border directives often only exist for emergency cases but not for everyday security systems. However, the latter can be seen as even more relevant for a security policy, since it accounts for the majority of the incidents. In some French border regions a cross-border support, for example in emergency rescue and fire protection, is already established at the operational level. Yet, in addition to technical administrative and organisational interoperability, tactical interfaces must be compatible to foreign systems too. This is difficult in security since the national designs often differ. Since protection is perceived as a public or governmental task, the national organisation is influenced by political and administrative aspects. Nevertheless, private actors will continue to be involved in these tasks more and more. The harmonisation of national standards thus not only relies on a leveling, but a dynamic development that builds upon proven principles and structures. While a cross border exchange and transfer of knowledge in the development of emergency response systems has been initiated in France a while ago, the comparison between neighboring countries e.g. Germany still shows different designs of emergency response systems and its functioning. For instance, in the discussion about disaster prevention in France, it is repeatedly demanded that the federal government should take the lead role to coordinate everything centrally. Here, unfortunately, little is known whether and at what damage and event size the interaction of federal and provincial governments is preferable. In this regard countries can learn from each other or even adapt solutions from its neighboring countries. One example is the 45,000-strong German Federal Agency for Technical Relief (THW) which was the example model for building a civil defense unit in France.179

3.3.4. THE SECURITY CONFORMITY ASSESSMENT FRAMEWORK

Accredited certification indisputably demonstrates compliance in a security system. Validate competence and relevance of a quality organisation is a strong commitment. This is why the process leading to accreditation is so rigorous. The steps involved in accreditation are multiple: preliminary analysis of demand, definition of the evaluation programme, the constitution of the evaluation team, evaluating, writing and analysis of the report, finally, decision and delivery of accreditation. Accreditation is granted for an entire business or for an indefinite period. It is obtained for a domain or skill specific geographic sites and renewable term, which will take place during regular surveillance audits.

COFRAC (Comité français d'accréditation)

In France the accreditation body COFRAC (Comité français d'accréditation) is the organisation in charge of any accreditation activities. COFRAC was created in 1994 under the Act of July 1, 1901 and has been designated as single national accreditation by the Decree of 19 December 2008, in recognition of accreditation as a public authority activity. All interest related to accreditation are represented in the General Assembly and the Board of Directors and all decision-making bodies. COFRAC distributed as follows among 3 colleges present to the Board of Directors and the General Assembly: 1. Accredited agencies or their representative groups 2. Business professional groups or persons or structures of buyers using or may use the services of agencies. 3. Public interest representatives (government, state agencies, national institutes, consumer associations, users or the environment) for providing a sovereign function and the defense of collective interests. Qualified persons are admitted as associate members. COFRAC employs a permanent team of more than 130 employees. Four sections manage accreditations:

- Section 1: Laboratories, itself composed of four divisions: Biology-Biochemistry, Chemistry and Environment, Mechanics, Physics and Electrical Inspection
- Section 2: Inspection
- Section 3: Certifications
- Section 4: Human Health

About 200 quality controllers and evaluators and over 1,100 technical evaluators are regularly commissioned by COFRAC. Around the permanent structure: an internal audit committee regularly reviews the functioning of accreditation and compliance by COFRA with the requirements for accreditation bodies and four sectional committees, corresponding to the 4 sections of accreditation. 7 commissions (CTA) Accreditation of Laboratory Techniques are attached to the section committee which is structured in: Biology and Food Chemistry-Environment, Inter-laboratory Comparisons and Reference Materials, Mechanical, Thermal, Civil Engineering Building and Information Electricity-radiation-Technologies such as Legal Metrology.

In 1994, year of establishment COFRAC, the government aimed to create a "Euro-compatible" system, in line with European and international practices for accreditation of conformity assessment bodies for promoting mutual recognition of services provided by accredited entities. COFRAC is therefore at the top of the building wanted by the authorities in the pyramid of trust: Certify that accredited organisations are competent and impartial, obtain international acceptance of their services and the recognition of skills laboratories, inspection
bodies and certification: this is the double mission COFRAC, French Accreditation Committee, conducted in accordance with national regulations and EU directives.

As the major player in the conformity assessment, COFRAC enjoys the confidence of the government, its partners, accredited organisations and their clients. All adhere to accreditation, convinced of its added value: legitimized competence, economic confidence, international recognition opening the doors for export.

**The French accreditation process**

In general the process of accreditation can be divided in 4 phases:

**Analysis**
- Formalization of the request
- Consideration of the admissibility of the case
- Establishment of an agreement between the applicant and COFRAC

**Evaluation**
- Definition of the evaluation programme
- Constitution of a suitable evaluation team
- Evaluation

**Decision Making**
- Examination of the evaluation report in an ad hoc committee
- Formulation of an opinion for decision

**Notification**
- Notification of the decision by the director of COFRAC
- Issue of a certificate specifying the scope and duration of accreditation

The first accreditation or initial accreditation is granted for a maximum period of 4 years. Throughout this cycle of 4 years, each organisation is regularly assessed (on average every year) during follow-up assessments called feedback of surveillance. At the end of this period of 4 years, the accredited body is subjected to a renewed evaluation after which accreditation is renewed on success for a further period (5 years maximum).

Figure 23 lists all certification bodies accredited by COFRAC for the fields of "sûreté" and "security". The accreditation specifies all activities of certification as well as the domain of operation. Accredited certification bodies must transparently provide such information since accreditation is not connected the certification body itself but for the activities involved as well as the domain of activity.
<table>
<thead>
<tr>
<th><strong>Accredited CAB:</strong></th>
<th><strong>For:</strong></th>
<th><strong>In the domain:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>AFNOR Certification</td>
<td>div.</td>
<td>e.g. alarm systems, installation services of CCTV systems&lt;sup&gt;180&lt;/sup&gt; see next chapter</td>
</tr>
<tr>
<td>Bureau Veritas Certification France</td>
<td>div.</td>
<td>e.g. installation services of CCTV systems&lt;sup&gt;181&lt;/sup&gt;</td>
</tr>
<tr>
<td>RAPT-Unité EST/ISF/QS/AQL</td>
<td>activities of testing/calibration</td>
<td>Electronic, Computing and Telecommunications Systems, Software</td>
</tr>
<tr>
<td>CNPP Entreprise / CNPP CERT</td>
<td>Type C body&lt;sup&gt;182&lt;/sup&gt;</td>
<td>e.g. safety of the People and the Goods including installation services of CCTV systems&lt;sup&gt;183&lt;/sup&gt; see next chapter</td>
</tr>
<tr>
<td>SONOVISION</td>
<td>Type C body</td>
<td>Safety of the People and the Goods</td>
</tr>
<tr>
<td>ESP Conseil</td>
<td>Type C body</td>
<td>Safety of the People and the Goods</td>
</tr>
<tr>
<td>Société d'Assistance en Pyrotechnie-SAP</td>
<td>Type C body</td>
<td>Safety of the People and the Goods, Environment</td>
</tr>
<tr>
<td>Service Technique de l'Aviation Civile (STAC)</td>
<td>activities of testing/calibration</td>
<td>e.g. Security / Airport Security Equipment, Building and Civil Engineering /</td>
</tr>
<tr>
<td>Autorité de Sureté Nucléaire (ASN)</td>
<td>Type A body&lt;sup&gt;184&lt;/sup&gt;</td>
<td>Pressure Equipment - TDG – Pipeline</td>
</tr>
<tr>
<td>Institut de Radioprotection et de Sûreté Nucléaire (I.R.S.N.)</td>
<td>activities of testing/calibration as well as inter-laboratory comparisons</td>
<td>Security / Personal Equipment Providing General Body Protection, Security / Devices used for the Radiation Protection, Ionizing Radiation, Food and Food Products / Foodstuffs,&lt;sup&gt;185&lt;/sup&gt; Air Quality - Water Quality&lt;sup&gt;186&lt;/sup&gt;</td>
</tr>
<tr>
<td>LCIE</td>
<td>activities of testing/calibration</td>
<td>e.g., Electronic, Computing and Telecommunications / Data Processing Devices and Audio Video Apparatus - Telecommunication Equipment, see next chapter</td>
</tr>
<tr>
<td>LSTI</td>
<td>div.</td>
<td>e.g. security services&lt;sup&gt;187&lt;/sup&gt;</td>
</tr>
<tr>
<td>Centre Scientifique et Technique du Bâtiment (CSTB)</td>
<td>activities of testing/calibration</td>
<td>e.g. Building and Civil Engineering / Construction Components, Public Road and Environment Components - Public Road Equipment and Road Environment Equipment, Aeronautic Equipment</td>
</tr>
<tr>
<td>Schneider Electric Industries SAS</td>
<td>activities of testing/calibration</td>
<td>e.g. All Electrical and/or Electronical Equipment or Products Subject to Fire Behaviour Testing, Industrial Equipments and Engineering Products</td>
</tr>
</tbody>
</table>

<sup>180</sup> Certification des installateurs de systèmes de vidéosurveillance prévue par l'arrêté du 5 janvier 2011, see https://www.cofrac.fr/fr/organismes/

<sup>181</sup> Certification des installateurs de systèmes de vidéosurveillance prévue par l'arrêté du 5 janvier 2011, see https://www.cofrac.fr/fr/organismes/

<sup>182</sup> Provides other inspection services than “third party” to its parent organisation or to other clients

<sup>183</sup> Certification des installateurs de systèmes de vidéosurveillance prévue par l'arrêté du 5 janvier 2011, see https://www.cofrac.fr/fr/organismes/

<sup>184</sup> Provides exclusively “third party” inspection services

<sup>185</sup> Security of the society also includes food security

<sup>186</sup> Relevant regarding drinking water infrastructure

<sup>187</sup> Certification des prestataires d’audit de la sécurité des systèmes d'information (PASSI) based on NF EN 45011 / NF EN ISO/CEI 17065 - Services
<table>
<thead>
<tr>
<th>Laboratories Pour-query</th>
<th>activities of testing/calibration</th>
<th>e.g. Transport / Road Vehicles and Equipments, all Electrical and/or Electronical Equipment or Products Subject to Fire Behavior Testing, Food and Food Products / Food Contact Materials</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNRS</td>
<td>Type A body</td>
<td>Health(^{188})</td>
</tr>
<tr>
<td>SGS ICS</td>
<td>div.</td>
<td>e.g. Services certification concerned by French Regulations, Certification by type testing of medical Prescription assistance software for ambulatory medicine; IFS Food certification; Food products certification</td>
</tr>
<tr>
<td>Cesame Exadebit SA</td>
<td>activities of testing/calibration</td>
<td>Included in the database without mentioning specific security domains</td>
</tr>
<tr>
<td>CETIM</td>
<td>activities of testing</td>
<td></td>
</tr>
<tr>
<td>Eurocontrol Odif</td>
<td>activities of testing/calibration</td>
<td></td>
</tr>
<tr>
<td>CNRS</td>
<td>Type A body</td>
<td></td>
</tr>
<tr>
<td>LCIE</td>
<td>activities of testing/calibration</td>
<td></td>
</tr>
</tbody>
</table>

Note: The original search was word “Sûreté”. The database output was refined by the authors, several entries, which do not seem to describe security topics, were removed; additional entries were included based on searches per specific accreditation standard.

Figure 23: Accredited certifications from COFRAC in the security field

### 3.3.5. **SELECTED SECURITY CERTIFICATION BODIES AND THEIR WORK**

Security certification ensures certainty of the functioning of different security related systems. The certification process tests whether the level of comfort, equipment reliability and ease of use meets certain criteria. Certified products stand out and can be differentiated from others by the consumer. In France several certification bodies exist where teams of experienced auditors assess conformist to security standard, but also through practical cases from real situations auditing the system, product or service in questions. In France security certification is connected to different security topics. Figure 24 illustrates the number of French certification schemes that exists for the topics: Management system certification (9 certificates), Product certification solutions (33 certificates), Service certification solutions (5 certificates), Competency certification solutions (7 certificates), Assessment (3 certificates), Tests (1 certificate) Regulatory statement (10 certificates).

---

\(^{188}\) Critical infrastructure also includes health infrastructure
In the following, we illustrate and briefly describe different security certification schemes in France the topics that relate to the schemes and the security standards that ensure compliance.

**AFNOR—Association Française de Normalisation**

AFNOR Certification is the first certification body and evaluates systems, services, products and people in France. AFNOR assesses performance to recognise the quality of its organisation, products, services or skills of men and women who make up its teams with more than 500 products. AFNOR Certification is one of the most comprehensive on the market. In the following we provide information on selected security certification schemes conducted by AFNOR. A specific focus will be put on intrusion detection equipment, NF and A2P marks.

Certified products are marked with the NF and A2P marks for identification and traceability. The NF mark is owned by AFNOR, indicating conformity with French, European and international standards. The A2P mark is a non-compulsory certification mark and distinguishes intrusion detection systems and fire protection equipment. The two marks shall not be separated on electronic security products. The applicant of the mark has to ensure the traceability and shall market the certified products itself. Furthermore, the applicant has to be in control of certain product development phases. In particular, these phases relate to the design of the product, the procurement of the raw materials, the manufacturing of the sub-assemblies as well as the assembly of the finished product, the product inspection and finally the marking of the product.

**Management system certification**

- **ISO / IEC 27001**
  - **Related topics:** Certification meets the challenges organisations in terms of protection of information, relevant customer requirements and areas of regulatory compliance, and increasingly competitive markets. Information is an essential asset in an organisation and can be of strategic importance according to its nature and content.
- **Evaluation criteria:** Interview and gather information about the client’s organisation, his environment and management system. Completion of the certification audit: Step 1: preliminary analysis of the essential elements of the client’s management system, Step 2: audit of his business and practices by conducting interviews, review of indicators, etc. Drafting of an audit report. Taking certification decision. Issuance of the certificate for 3 years. Achievement of annual or semi-annual surveillance audits.

- **Security solutions:** Identify the critical information of the organisation, define protection and appropriate response measures, implement a security management system for coherent and effective information, define new patterns of consumption and dissemination of information, ensuring that organisations better organise and monitor security objectives; and thus perform better in security and in the management of security.

- **International Agreements:** AFNOR security certification builds on the principles of the process approach and the PDCA (Plan-Do-Check-Act), ISO / IEC 27001 fits naturally in organisations having or wishing to implement management system procedures (quality or environment, etc.). Thus AFNOR Certification carries out various combinations of certifications audits according to the client’s wishes on the basis of ISO/IEC 27001: ISO 9001, EN 9100, ISO 14001, ISO/IEC 20000-1, CMMi

**Product certification solutions**

- **NF - Fire resistant doors** – Related topics: the swinging door: Door-block, single or double leaf, pivoting about a vertical axis side sliding door: Door, horizontal translation and single or multiple leaf hinged or not the curtain and door-to-pull-off vertical: Device vertical translation self-closing in the bay plan to close with winding (curtain) or without winding (door to pull-off vertical, horizontal or vertical open position).


- **NF Electronic Security Equipment – Intrusion Detection – Access Control Management Equipment** (see ‘Specific example’ below)

**Service certification solutions**

- **NF Service - Private prevention and security services**
  - **Related topics:** In-house inspection of the service. Related standards: NF X50-777 (19980501). Service Commitment - QUALISECURITE - Service Delivery private enterprises human supervision - REF215. Provide specific buying criteria to contractors, professionalize human surveillance companies, clarify the customer / provider relationship by creating a common reference language.
  - **Security solutions:** Prevention and Security Service for Home, Commercial offer, Sale. Preparation and implementation of the service, Following instructions, Organisation of the service, Staff Training, Management of customer satisfaction, Internal control delivery
Specific example: AFNOR-- NF 324-H58  
Electronic security equipment - intrusion detection equipment

The certification scheme relates to electronic security equipment of intrusion detection as well as to access control management equipment. The certification rules cover several product families in the field of intrusion detection e.g. Control and Indicating Equipment and Phone Transmitter, Control and Indicating Equipment, Control and Indicating Equipment Alarm transmitter and others. The certification rules also cover several product families in the field of access control systems for use in security application e.g. Access Control Supervising Processing Unit (ACSPU), Access Control Processing Unit (ACPU), Local Processing Unit (LPU), reader and associated identifiers and others.

The certification rules define a list of essential certified characteristics. These characteristics relate to the inclusion of certain functions or the benchmark criteria of ranges e.g. the environmental class (e.g. I, II, III, and IV), the number of recorded events, time duration, power supply type, the stand-by time, the number of loops, ranges or opening angles. The certification rules further describe certain requirements in terms of quality organisation. The requirements relate to the identification of processes, documentation, communication, resource management such as monitoring and measurement. Applicants of the mark also have to follow certain provisions concerning the product manufacturing which include e.g. checks on the equipment parts list, inspections or sample tests. The NF and AP2 mark are further associated with one or more shields which reflect the overall security level of the product and its autonomy for intrusion detection systems and the level of access and autonomy in access control management equipment. The shield logos provide visual information about the characteristic for certified products. Marks on non-compliant products have to be removed. Certified products must be accompanied by a so called technical file indicting the characteristics of each product. The file must be at least in French and has to contain the commercial reference, name and address of license holder and certification body, certification rules and characteristics, instructions for use and maintenance as well as installation instructions.

The certification scheme lists the acceptance procedures for obtaining the certification of a product ranging from requirements of application to the extension of a certificate and rules for maintaining and piggybacking a mark. Furthermore, the scheme describes monitoring procedures for maintaining the certification like audit procedures, inspections, third party product control, checks after lawsuits, claims or disputes and modifications. In cases of removal of the mark in the event of sanctions or nonconformities the license holder has to fulfil certain conditions e.g. such as stop to deliver the non-compliant products, ensure reparation, withdraw the mark taking all measures required to identify the lots in question.

The certification scheme lists all stakeholders involved in the management and operation of joint NF and A2P certifications such as e.g. laboratories, committees or audit bodies. Finally the scheme describes the nature of the services relating to NF and A2P certification and the methods of payment is in terms of fees for the license holder, the trademark, commercial reference, audits, tests and checks.

Like CNPP, AFNOR belongs to EFSG and collaborates with other European certification bodies in the security field. The section on CNPP will describe this in more detail.
LCIE -- Laboratoire Central des Industries Electriques

LCIE assesses compliance of electrical and electronic products to national security marks. LCIE Bureau Veritas solutions help to ensure the quality and safety of products throughout the world. With years of experience in electrical and electronic equipment, the LCIE accreditations demonstrate compliance with the following standards in force: for testing activity: NF EN ISO / IEC 17025, for the activity product certification: EN 45011 - ISO IEC Guide 65, for business activity and personal certification: EN ISO / IEC 17021. In the following we proved information on selected security certification schemes conducted by LCIE.

International Agreements: The European ECS Agreement enable the granting of the ENEC (European Norms Electrical Certification), HAR (Cables and conductors) and EMC (Compliance with the electromagnetic compatibility standards) marks. ASEFA issues the LOVAG (Low Voltage Agreement GROOP) for European compliance Type Certificate or Mark for electrical and electronic products. The GS Mark to access the German market: The GS mark is a voluntary mark indicating that some products are meeting safety requirements. The issuing and management requirements of the mark are detailed in the German Equipment and Security Act (GPSG or "Geräte- und Produktsicherheitsgesetz") dating back to 01/06/2004 and relating to Technical Work Equipment and Consumer Products.

Product certification solutions

- **NF - Autonomous electrical security equipment**
  - Related topics: Electronic security equipment, intrusion detection and access control monitoring equipment. This certification is particularly electronic security products wireline technology intrusion detection, radio or mixed; access control management equipment and smoke generators (as to NF015).
  - Evaluation criteria: Rated supply voltage, Nominal characteristics of the output voltage, Rated power, Operating characteristics, Class of protection against electric shock I, II, and III, Classification according to the degree of protection against ingress of dust, solid objects and moisture, Resistance to shock, Level of the sound signal general alarm indicated by the class A, B, C, D, where applicable, the type Pr, Sa, Ma, RSS assigned, RSS 5 minutes, Permanent or non-permanent operating mode.
  - Security solutions: Power supplies storage batteries, self-blocks alarm emergency evacuation, autonomous blocks security fluorescent lighting, blocks autonomous emergency lighting to incandescent lamps, blocks autonomous emergency lighting to incandescent lamps for residential building, portable autonomous blocks intervention, self-box power for emergency lighting powered by central source, central source luminaires, automatic test system for emergency lighting devices.

CNPP - Centre national de prévention et de protection

CNPP certifies prevention and risk control and develops, disseminates and evaluates the knowledge and expertise of people in security, tangible and intangible heritage, the environ-
ment in all activities and all backgrounds. In the following we proved information on selected security certification schemes conducted by CNPP.

**International Agreements:** CNPP’s is accredited by COFRAC concerning its certification activities from industrial products under the A2P mark, CE conformity evaluation/marking, quality management systems incompliance with the ISO 9001 : 2008 and to some of specific service certifications under the APSAD mark. Furthermore CNPP is member of the EFSG (European Fire and Security Group) and in this regard cooperates with ECBS, SBSC and VdS under the “High security locks” and the “Safes and strongrooms” agreement. In addition, CNPP cooperates with LPCB, VdS and AFNOR under the “Alarm Systems components” agreement.

**Product certification solutions**

- **NF - Electronic security equipment, intrusion detection and access control monitoring equipment**
  - **Related topics:** Performance of IP and IK envelopes, fraud (type 1, 2 or 3). Other features are presented in the certification rules. This certification is particularly electronic security products wireline technology intrusion detection, radio or mixed; access control management equipment and smoke generators (as to NF015). These include: Alarm Central; Central alarm with alarm transmitter;
  - Telephone transmitter; Infrared Motion Detector (passive or active); Shock sensor; Opening detector contact; Sensor shock and openness and Seismic Detector; related standards: - No standards associated.
  - **Security Solutions:** Ability to function, IP and IK envelopes, fraud ability (type 1, 2 or 3), Detection and alarm systems, Video surveillance, Safes and banking systems, Locks and building protection, Extinguisher systems and extinguisher agents, Smoke extraction systems, Infrared thermal imaging, Vehicle antitheft systems

**3.3.6. SUMMARY AND CONCLUSION**

France is an active player and contributor to European and international security-related standardisation that has several good practices that support the connection between various stakeholders of security solutions. Strong examples include: the ‘Security Forum’ at AFNOR, which is working to determine the minimum conditions of interoperability in order to more directly exploit sources of video; the French GIS, ‘Group d’ Impulsion Stratégique’, which has the aim to strengthen the French position in international security standardisation; and the cooperative arrangements between AFNOR, CNPP and other European certification bodies.

Despite the strong efforts towards interconnectedness demonstrated by France, several issues must still be addressed, particularly as they related to cross-national interoperability, in order
to ensure citizen security. To date, there are few specific cross-border directives and those that do exist only for emergency situations. This may be a challenge as the technical, administrative and organisational structure of security systems are based on unique national designs, effectively obstructing cohesion. In response to the fact that security is considered a government task, albeit there is no general consensus as to which level of conditions warrant government intervention, innovate measures that work to harmonize national standards by building upon proven practices are essential – especially as efforts to develop and implement a new EU standard for security services ensues. In this respect, EU countries can learn from each other or adapt to solutions presented by other Member States, as was the case of ISO/PAS 22399. Efforts in this respect will be further challenged by the constraints of time and resources.

### 3.3.7. References


3.4. **GERMANY**

3.4.1. **INTRODUCTION**

Germany is one of the biggest players in the European market for security PSS. In addition to various security companies, in different market segments on the demand side for certification, there is also a multifaceted landscape of security conformity assessment bodies.

This country study is based on a mix of methods and sources. Interviews with respondents at standards and certification bodies were used to answer specific questions, which build on guidelines developed by CRISP partners and in order to identify relevant certification bodies, the database of the national German accreditation body DAkkS was used. The 55 search results led to further analyses and selection. Different market surveys were analysed to describe the German market for security solutions. Further desk research included the analysis of standards by using the database Perinorm and the search engine of the Beuth Verlag. A meeting at the DAkkS helped to verify selected research results.

3.4.2. **SHORT DESCRIPTION OF GERMANY’S SECURITY INDUSTRY**

**Introduction**

Germany is an important player in the European and worldwide security market. As illustrated in Figure 25, different estimations of its market volume and characteristics range from € 3 bn in 2010 to 31 bn in 2015. These differences can be attributed to several reasons, e.g., the year of reference, the methods of data collection and the definition of the ‘Security Industry’ which was applied to determine the inclusion of companies.

Most data presented here are obtained from the Market Survey 2012 by the Brandenburg Institute for Society and Security (BIGS), which refers to the year 2011 and associated follow-up surveys from 2013 and 2014.

The study is very inclusive and builds up on a definition of the Security Industry including “all companies that offer products and services for the protection of critical infrastructure, protection against crime, industrial espionage and terrorism, the protection of persons and the management of crises and (natural) disasters”. In the 2012 study telephone interviews with a net sample of 696 companies were analysed and extrapolated. In the follow-up study, data were collected by means of surveys of 230/150 participants and the companies were di-

---

189 Interview questions can be found in chapter 3.4.9
191 The Beuth Verlag is responsible for the dissemination of standards in Germany, in particular for DIN, EN, ISO and IEC standards.
194 BIGS, op. cit., 03/2015
195 BIGS, op. cit., 03/2015, p. 2.
vided into the industry sectors “Security Products and Technologies”, “Security Services” and “IT-Security”.

<table>
<thead>
<tr>
<th>Source/Study</th>
<th>Title</th>
<th>Market Volume in S/€</th>
<th>Year of Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>WiFOR (2012)</td>
<td>Quantifizierung der volkswirtschaftlichen Bedeutung der Sicherheits- und Verteidigungsindustrie für den deutschen Wirtschaftsstandort</td>
<td>28.3 bn €</td>
<td>2011</td>
</tr>
</tbody>
</table>

Source: BIGS
Figure 25: Estimation of the turnover of the German security industry based on different studies

Additional figures build on a report from 2009 by VDI/VDE-IT\(^{196}\) as presented by Germany Trade and Invest (GTAI).\(^{197}\) That study used a mix of methods including review of secondary literature, portfolio analyses and interviews with a smaller sample of experts.

**The company landscape**

Germany’s supply side of the security market includes many large and established international companies, for example, Siemens, Bosch and Smiths Heimann. However, the majority of the companies in the market are small and medium-sized enterprises. Overall, 450,000 people are employed in the security industry.\(^{198}\) The fact that one third of the companies were founded after 1999 demonstrates that the vendors of security solutions belong to a rather young industry. This is especially true for IT security and security services.\(^{199}\) Another interesting aspect is the offering structure of the companies and the high rate of companies offering not exclusively product but also services. For example in the 2014 BIGS survey it was found that the overwhelming majority (>80 %) of IT-security companies offer either exclusively services, or both services and products (all other security companies: 70%).\(^{200}\) In general, the German security industry is characterised by a combination of innovative components manufacturers, mostly SMEs, and system vendors who integrate these components to

---


\(^{198}\) BIGS, op. cit., 03/2015, p. 6.

\(^{199}\) BIGS, op. cit., 03/2015, p. 5.

\(^{200}\) BIGS, op. cit., 03/2015, p. 4f.
D2.2: Consolidated report on security standards and certification

The companies are organised in a variety of security associations and networks, which are shown in the annex. The demand side of security solutions consists of public actors, private enterprises and citizens. On average the latter are responsible for 16%, public actors for 24% and private enterprises for 60% of the demand.\(^{201}\)

**Turnover of the security industry**

The 2012 BIGS survey estimated the turnover of the German Security Industry to be € 35 bn in 2011. The following figure shows the importance of different market segments in 2009 based on the result by VDI/VDE-IT referring to an estimation of turnover of € 20 bn.

Sources: GTAI\(^{203}\) and VDI/VDE-IT 2009

Figure 26: Security turnover in Germany by technology segments

According to the figure, break-in prevention has the biggest market share, followed by IT security, equipment and emergency communication.

**Export and internationalisation**

The 2012 BIGS survey came to the result that the international market plays an important role for Germany’s security companies. The share of companies that were active mostly on the regional markets sank from 48% to 31% within a two year-period while the percentage of


companies active on the international market increased to 30%. A trend towards activity on markets with a bigger geographical scope can be observed.

3.4.3. THE SECURITY STANDARDISATION FRAMEWORK

The key player in the German standardisation landscape is the DIN, the German Institute for Standardisation, which is a private organisation registered as a non-profit association. Its members come from industry, associations, public authorities, commerce, the trade and research organisations. By agreement with the German Federal Government, DIN is the acknowledged national standards body that represents German interests in European and international standards organisations at CEN and ISO.

The DKE German Commission for Electrical, Electronic & Information Technologies of DIN and VDE is the national organisation responsible for the creation and maintenance of standards and safety specifications covering the areas of electrical engineering, electronics and information technology in Germany. The DKE is the German member of the IEC International Electrotechnical Commission and CENELEC European Committee for Electrotechnical Standardisation. It is also the national standardisation organisation (NSO), responsible for Germany at ETSI, the European Telecommunications Standards Institute. The European and international activities of both institutions are shown in Figure 27.

<table>
<thead>
<tr>
<th>Area</th>
<th>Geographic Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>national</td>
</tr>
<tr>
<td>General</td>
<td>DIN</td>
</tr>
<tr>
<td>Electrical and electronic technologies</td>
<td>DKE</td>
</tr>
<tr>
<td>Information and telecommunication</td>
<td>DKE</td>
</tr>
</tbody>
</table>

Source: DIN e.V.
Figure 27: DIN’s and DKE’s involvement in European and international standards development

The names of standards from DIN and DKE start with the acronym “DIN”. In addition to formal standardisation leading to standards based on consensus, DIN offers the opportunity to develop specifications based on so called “informal” or “consortia” standardisation. A speci-

---

204 BIGS, op. cit., 03/2015, p. 10.
206 VDE, “The mandate of the DKE”, no date. http://www.vde.com/en/dke/Aboutourselves/Pages/The%20Mandate%20of%20the%20DKE.aspx;
D2.2: Consolidated report on security standards and certification

CRISP project

A portal was created to facilitate the coordination of this work. DIN describes the relevant standardisation process as follows:

“Within cooperative standardization involvement of all so called interested parties is not required. Therefore a head start in comparison to the formal and consensus based standardization process occurs. Particularly in highly innovative fields this head start pushes the knowledge and technology transfer of your innovation.”

Specifications can be used as a basis for consensus based standardisation later on. All DIN specifications are marketed under the product type “DIN SPEC.”

In addition, Germany is a significant contributor to/and adopter of international and European standards. Database research on the website of DIN led to the following results: 1728 hits for the word ‘security’, 1,134 specific hits after refining the search by adding ‘DIN’ and specific 688 hits for German documents. An analysis of the hits led to a substantial number of datasets, which are relevant in CRISP’s context. Most documents are DIN SPECs. Like CWAs, they have a short life and can therefore not be used for certification. Nevertheless they can form the foundation of German and even European standards. The following lists show DIN Normen and DIN SPECs with specific relations to conformity assessment, supplemented by DIN Normen and SPECs, which consider additional security issues. For simplicity’s sake, they only include documents developed in Germany and no national versions of European or international standards such as DIN EN standards or DIN EN ISO standards.

DIN Normen and DIN SPECs, which offer specific criteria for conformity assessment

- DIN 77200 2008-05 Sicherungsdienstleistungen – Anforderungen / Static guarding and mobile patrol services -Requirements
- DIN 6878-1 Digitale Archivierung in der medizinischen Radiologie - Teil 1: Allgemeine Anforderungen an die Archivierung von Bildern
- DIN 18650-1 Powered pedestrian doors - Part 1: Product requirements and test methods
- DIN 31644 Information und Dokumentation - Kriterien für vertrauenswürdige digitale Langzeitarchive
- DIN 6789 Dokumentationssystematik - Verfälschungssicherheit und Qualitätskriterien für die Freigabe digitaler Produktdaten

---

DIN 18104-1 Einbruchhemmende Nachrüstprodukte - Teil 1: Aufschraubbare Nachrüstprodukte für Fenster und Türen - Anforderungen und Prüfverfahren

DIN 18104-2 Einbruchhemmende Nachrüstprodukte - Teil 2: Im Falz eingelassene Nachrüstprodukte für Fenster und Türen - Anforderungen und Prüfverfahren

DIN 25422 Aufbewahrung und Lagerung radioaktiver Stoffe, Anforderungen an Aufbewahrungseinrichtungen und deren Aufstellungsräume zum Strahlen-, Brand- und Diebstahlschutz

DIN SPEC 27009 Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002

DIN SPEC 91297:2013-12, Titel (englisch): Attribution of a certificate based on a specific role model for the Internet of energy (energy security services)

DNVGW G 1000 Anforderungen an die Qualifikation und die Organisation von Unternehmen für den Betrieb von Anlagen zur leitungsgebundenen Versorgung der Allgemeinheit mit Gas (Gasversorgungsanlagen)

DVGW W 1000 Anforderungen an die Qualifikation und die Organisation von Trinkwasserversorgern / Requirements on the qualification and organisation of drinking water suppliers

In particular DIN SPEC 91297:2013-12 offers interesting features related to certification because it describes attributes which a certificate in a specific security area should have.

Other DIN Normen and DIN SPECs in the security field

DIN 66274-1 Informationstechnik - Internet-Zugänge - Teil 1: Begriffe

DIN 16560-16 EDIFACT - Anwendungsregeln - Teil 16: Anwendung des Service-Nachrichtentyps KEYMAN zur Übermittlung von Sicherheitsschlüsseln und – zertifikaten

DIN SPEC 91293:2013-05, Titel (englisch): Security Modeling Technique (SMT) for visualizing and analyzing security relevant information based on security levels

DIN SPEC 91282:2012-11, Titel (englisch): Terminology for security management transport infrastructures

DIN SPEC 91287:2012-07 (E) Data interchange between information systems in civil hazard prevention

DIN SPEC 91296 Klassifizierung von Gefährdungen für Gebäude infolge von Terrorismus

DIN SPEC 66286 Management von Cloud Computing Lösungen in kleinen und mittleren Unternehmen (KMU)

DIN SPEC 91213-1 Open Traffic Systems - OTS 2-Schnittstellenspezifikation - Teil 1: Einführende Erläuterungen für Entscheidungsträger

DIN SPEC 91213-2 Open Traffic Systems - OTS 2-Schnittstellenspezifikation - Teil 2: Technische Spezifikation für Implementierer

DIN 14675 Brandmeldeanlagen (Aufbau und Betrieb) / Fire detection and fire alarm systems – design and operation


DVGW G 1001 Sicherheit in der Gasversorgung - Management von Risiken im Normalbetrieb

DVGW G 1002 Sicherheit in der Gasversorgung - Organisation und Management im Krisenfall
• DVGW W 1001 Sicherheit in der Trinkwasserversorgung - Risikomanagement im Normalbetrieb / Safe and Secure Drinking Water Supply - Risk Management Under Normal Operating Conditions

Germany also has a specification, which provides data protection guidelines. The PAS 1011 VCS communication approaches to healthcare includes, based on the work of the Hamburg data protection supervisor, four categories of data that are organised in ascending order from the perspective of confidentiality. Based on a classification of the data to be protected in one of these categories, to protect the data different measures in the specification are recommended or prescribed.

Data of the stages B to D are associated with specific privacy risks, which, however, usually have a connection to stage A data, in particular the name of the person. Special measures for data protection in the different stages are not specified in the PAS 1011. Specific security-related data such as video and fingerprint data, obtained by data from iris-scanning or data combinations are not considered in the PAS 1011.

Additional German security standards, which are in most cases more focused on safety aspects, are shown in the Annex of the Mandate M/487 to Establish Security Standards, Final Report Phase 1 Analysis of the Current Security Landscape. Figure 28 shows Germany’s involvement in international security-related standardisation activities based on twelve examples.

### Public organisations

A key public organisation in Germany’s security standardisation landscape is the Federal Office for Information Security (BSI), which is the country’s national cyber security authority. The BSI develops own guidelines, which are available on its website. BSI guidelines that specify privacy and data protection aspects also exist. Examples are shown below:

- BSI/TR 03104 VR3, TR PDÜ hD Technische Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für hoheitliche Dokumente; Version 3.2.2
- BSI/TR-03123 Technische Richtlinie – XML-Datenaustauschformat für hoheitliche Dokumente (TR XhD)
- BSI/TR 03126-1: Einsatzgebiet “eTicketing im öffentlichen Personenverkehr“
- BSI/TR-03132 Technische Richtlinie – Sichere Szenarien für Kommunikationsprozesse im Bereich hoheitlicher Dokumente
- BSI/TR 03116 Technische Richtlinie für eCard-Projekte der Bundesregierung; Version 3.04.
- BSI/TR 03116-2 eCard-Projekte der Bundesregierung - Teil 2: Hoheitliche Ausweisdokumente

BSI’s certification services are presented in chapter 3.4.4.

---


ISO TC | Topic | Participation (P- Member, O-Member)  
--- | --- | ---  
ISO/IEC/JTC 1/ SC 17 | Cards and personal identification | P  
ISO/IEC/JTC 1/ SC 27 | IT Security techniques | P, Secretary  
ISO/IEC JTC 1/ SC 31 | Automatic identification and data capture techniques | P  
ISO/IEC/JTC 1/ SC 37 | Biometrics | P  
ISO/TC 68 | Financial services | P  
ISO/TC 85 | Nuclear energy, nuclear technologies, and radiological protection | P  
ISO/TC 92 | Fire safety | P  
ISO/TC 223 | Societal security | P  
ISO/TC 224 | Service activities relating to drinking water supply systems and wastewater systems - Quality criteria of the service and performance indicators | P  
ISO/TC 247 | Fraud countermeasures and controls | P  
ISO/PC 284 | Management system for quality of private security company (PSC) operations - Requirements with guidance | P  
ISO/TC 292 | Security | P  
Total P+O |  | 11  

Source: Own analyses  
Figure 28: Germany’s participation in selected ISO TCs  

**Other organisations**  
An important additional player, which defines technical guidelines in Germany, is the Association of German Engineers (VDI). In general, the VDI aims to promote innovation, efficiency and appropriate framework conditions for the industry. In addition, the association is an active standards developer. Approximately 200 standards are produced by VDI’s technical divisions annually and its set of technical regulations contains more than 2,000 valid VDI Standards, which extensively cover the broad field of technology. Today’s topics range from securing loads on road vehicles to testing of optical fibres. VDI’s website provides 25 standards and specific pages of standards based on the search word ‘security’. While most of the documents are related to IT security, one interesting document in the CRISP context is VDI 4065 Technique and organisation of operation security - Hazard evaluation - Guidance for the systematic proceeding.
3.4.4. The Security Conformity Assessment Framework

The legal framework of civil security is characterised by the ‘cross-cutting nature’ of this field and the central role of the state. Due to these characteristics, several relevant products are not covered by single European or national law. For some solutions such as fire alarm products, several laws and regulations exist, e.g. the Bauproduktenverordnung (BauPVO), the EMC Directive and the General Product Safety Directive 2001/95/EC.210 Regarding information and communication technologies, the regulatory framework also includes the IT Sicherheitsgesetz, the Signaturgesetz (Signature Act, SigG), and Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market, the European Electronic identification and trust services (eIDAS) regulatory environment as well as the German Data protection law (BDSG) and the Datenschutzgütesiegelverordnung (DSGSVO). Important guidelines are also IT-Grundschutz standards of the Federal Office for Information Security (BSI). As in many other countries, there is currently no national directive for the protection of critical infrastructure (water, energy, medical infrastructure etc.), but the scope and content of the IT Sicherheitsgesetz was currently extended to digital infrastructure, including critical infrastructures, such as energy and telecommunication infrastructure.211

According to the German accreditation body DAkkS, 55 organisations212 are accredited in the security (and safety) field, including six organisations for security products based on ISO/IEC 17065 and two based on EN 45011. The DAkkS database also includes 101 entries for the key word ‘alarm’ and 99 entries for ‘video’ (including internal laboratories of manufacturers). While there is no entry for the topics ‘privacy’ and ‘data protection’, there is one hit for the German translation ‘Datenschutz’. The relevant certification body is datenschutz cert GmbH.213 Information on this certification body will be given later in this chapter and in chapter 3.4.5.2. In addition, the description in section 3.4.5.2 will show that the term ‘accreditation’ is also used by additional organisations entrusted with specific security and data protection issues in the security field (e.g. by the Bundesnetzagentur and the Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein).

Besides private certification bodies, the organisations accredited by the DAkkS also include, for example, the Bundesamt für Informationssicherheit (BSI), the Federal Criminal Police Office (Bundeskriminalamt, BKA), Landeskriminalaemter (LKA), and other Police Organisations. In many cases, these organisations are certified for inspection or have certified internal laboratories. This means that they test security solutions regarding their eligibility for

210 Teichler et al., op. cit., 2013, p. 140.
212 Search for ‘security’ in the DAkkS database http://www.dakks.de/content/akkreditierte-stellen-dakks, the German word for ‘security’ is ‘Sicherheit’, which can also be translated as ‘safety’. The hits also include entries, which were classified as related to ‘Sicherheit’
213 Its accredited certificates build on the following documents: ‘ISO/IEC 27001:2013 information technology - IT security techniques - information security management systems - requirements i. V. m. ISO 27006:2011 information technology - service management - part 1: service management system requirements according to ISO/IEC 20000-1:2011 - requirements i. V. m. ISO/IEC 27006:2011 policy requirements for certification authorities issuing qualified certificates according to etsi ts 101 456 (electronic signatures and infrastructures according to - ESI) - requirements i. V. m. ETSI TS 119 403 v1.1.1 (2012-03) policy requirements for time-stamping authorities according to etsi ts 102 023 - requirements i. V. m. ETSI TS 119 403 v1.1.1 (2012-03) policy requirements for certification authorities issuing public key certificates according to ETSI TS 102 042 - requirements i. V. m. etsi ts 119 403 v1.1.1 (2012-03)” (source: DAkkS database)
the organisation’s own use in public security contexts while issuing additional certificates is not sought. Additional organisations, which certify critical infrastructure providers include, for example DVGW (Deutscher Verein des Gas- und Wasserfaches e.V. Technisch-wissenschaftlicher Verein), which is active in the field of water and energy infrastructure, as well as the Forschungsgemeinschaft Wind (FGW).

Private certification bodies

The largest certification organisations are TÜV Rheinland LGA Products GmbH, TÜV NORD CERT GmbH, DEKRA Certification GmbH, SGS TÜV GmbH and TÜV SÜD Industrie Service GmbH. Regarding the number of accreditations, each organisation had accreditations for 19-25 areas of certification in 2013. Specifically in the security field, other relatively big certification bodies are VdS and ECB. There are also associations, which are not accredited and offer certificate-like documents like BHE. A summary of the security-related conformity assessment services of these certification bodies is provided in Figure 29. According to an expert and additional sources, security certification providers with foreign headquarters active in Germany are for example UL (for security containers), Intertek, DNV and Bureau Veritas Germany.

The certification service providers are involved in many multinational collaboration activities. Nevertheless national standards are used for certification, too. An example provides the area of fire detection and alarm systems. At present, 1,246 installers for fire alarm systems are certified in accordance with DIN 14675 (SW, 2012). Although there is no regulation, which requires such a certificate, it is an essential requirement for market entry. Connecting systems without such a certificate with firefighting departments would be denied and insure such systems would be neglected or require very high fees. Therefore, installing a fire alarm system without being certified is de facto not possible and it is assumed that the number of certified companies covers almost the entire market. The installers are checked and certified by ten certification bodies in total. They include, for example, TÜV Nord, TÜV Rheinland, and the VdS. Each body is accredited by the DAkkS. The VdS claims to be the market leader, having certified about 75% of all installers.

According to Wurster et al., selected security-related TCs at CEN and CENELEC highlighted eight standards, which are relevant for certification. Additional standards were mentioned by security experts. Figure 30 shows the application of these standards in the German conformity assessment system.

---

214 Teichler et al., op. cit., 2013, p. 43.
217 Teichler et al., op. cit., 2013, p. 141.
218 The DAkkS database lists seven accredited certification bodies for DIN 14675 in April 2015. Additional information on certificates based on this standard are available at http://www.vaz-ev.de/index.php/zertifizierungsprogramme/arge-din-14675
219 Teichler et al., op. cit., 2013, p. 145.
<table>
<thead>
<tr>
<th>Certification of:</th>
<th>Security products</th>
<th>Security systems</th>
<th>Security services</th>
<th>Others</th>
<th>Basis of the testing and certification processes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Certification Body</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DEKRA</td>
<td></td>
<td></td>
<td>x (air cargo)</td>
<td></td>
<td>div.</td>
</tr>
<tr>
<td>DNV</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>See b)</td>
</tr>
<tr>
<td>DQS</td>
<td></td>
<td>x</td>
<td></td>
<td>x data protection</td>
<td>div.</td>
</tr>
<tr>
<td>ECB</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>div.</td>
</tr>
<tr>
<td>SGS</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>See c)</td>
</tr>
<tr>
<td>TÜV Nord Cert GmbH</td>
<td></td>
<td></td>
<td>x</td>
<td>X (processes)</td>
<td>div.</td>
</tr>
<tr>
<td>TÜV Rheinland</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td>See d)</td>
</tr>
<tr>
<td>TÜV SÜD</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>See e)</td>
</tr>
<tr>
<td>VdS</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>See f)</td>
</tr>
<tr>
<td>BHE</td>
<td></td>
<td></td>
<td>x</td>
<td>(companies)</td>
<td>See a)</td>
</tr>
</tbody>
</table>

a) Relevant national, European and/or international standards, own guidelines based on these standards, scheme BHE-certified specialist, BHE-certified planners

b) SOLAS/ISPS Code, according to the DAkkS, DNV is the only accredited CAB for EN 13094, EN 14025 and EN 12972 in Germany

c) e.g. ISO 22301 (Business Continuity Management), ISO 27001, ISO 28000, C-TPAT, TAPA standards (FSR, TSO, Cargo)

d) e.g. ISO 27001, ISO 18028, BSI Grundschutz, German Data protection law (BDSG)

e) Systems evaluation for LBA / EASA certification - Aircraft industry JAR-OPS / EASA, Flight schools JAR-FCL / EASA, Technical aviation company JAR-145 / EASA, Aircraft and Aircraft Equipment (e.g. ground equipment)

f) European and national standards, regulations, VdS guidelines, Prüfvereinbarungen, e.g. EN 1300, EN 1143, EN 14450, EN 54, EN 5013, DIN 14676

Figure 29: Overview of selected security-related certification bodies in Germany

Numerous additional documents are used for security certification including national, European and international standards from DIN, CEN, CENELEC, ISO, IEC and ETSI, VDE

---

221 Including IT security, risk management
223 The website of the company provides an overview of relevant markets which it addresses. The security industry is not included.
224 E.g. the airport Fraport but based on DIN EN ISO 9001. The certification also covers, for example, airport security management, see http://www.fraport.de/content/fraport/de/misc/binaer/nachhaltigkeit/zertifikate/fraport-group-iso-9001bis-07-2016/jcr:content/file/fraport-group-9001-de.pdf
225 Airport construction and aviation security
226 Including software, components, companies/service providers charged with the planning and design, engineering and installation of fire safety and security systems
227 Not accredited
228 Freight-Security-Requirements, truck safety requirements
229 Luftfahrt-Bundesamt / European Aviation Safety Agency
230 Joint Aviation Authorities
guidelines, CEA guidelines, guidelines from German certification bodies such as VdS, foreign standards (e.g. from the U.S. in exceptional cases) and guidelines from foreign certification bodies like for example from UL.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Number</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 28000 series</td>
<td>3</td>
<td>DNV Zertifizierung und Umweltgutachter GmbH, Germanische Lloyd SE Competence Centre Systems Certification, TÜV Rheinland Cert GmbH</td>
</tr>
<tr>
<td>ISO/IEC 27000</td>
<td>1</td>
<td>Test &amp; Integration Center (TIC) T-Systems Multimedia Solutions GmbH</td>
</tr>
<tr>
<td>IEC 62443</td>
<td>3</td>
<td>SGS-TÜV Saar GmbH, TÜV Rheinland InterTraffic GmbH, TÜV Süd Rail GmbH</td>
</tr>
<tr>
<td>IEC 62642</td>
<td>1</td>
<td>VdS</td>
</tr>
<tr>
<td>EN ISO 22301</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>EN ISO 27799</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>EN 13094</td>
<td>1</td>
<td>DNV GL SE Inspektions- und Zertifizierungsstelle für Werkstoffe, Produkte und Anlagen (DNV GL SE)</td>
</tr>
<tr>
<td>EN 14025</td>
<td>1</td>
<td>DNV GL SE</td>
</tr>
<tr>
<td>EN 12972</td>
<td>1</td>
<td>DNV GL SE</td>
</tr>
<tr>
<td>EN 14339</td>
<td>2</td>
<td>DVGW Technologiezentrum Wasser (TZW) Prüfstelle Wasser, DVGW CERT GmbH</td>
</tr>
<tr>
<td>EN 14384</td>
<td>2</td>
<td>DVGW Technologiezentrum Wasser (TZW) Prüfstelle Wasser, DVGW CERT GmbH</td>
</tr>
<tr>
<td>EN 50131</td>
<td>1</td>
<td>VdS</td>
</tr>
<tr>
<td>EN 50133</td>
<td>1</td>
<td>VdS</td>
</tr>
<tr>
<td>EN 50136</td>
<td>1</td>
<td>VdS</td>
</tr>
<tr>
<td>EN 50518</td>
<td>3</td>
<td>VdS, TÜV SÜD Industrie Service GmbH, TÜV Rheinland Industrie Service GmbH</td>
</tr>
<tr>
<td>EN 54 series</td>
<td>34</td>
<td>TÜV Nord, TÜV SÜD, VdS</td>
</tr>
<tr>
<td>EN 62676</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

Figure 30: German CABs related to selected security standards

**Federal organisations, organisations of Germany‘s Federal States and the public sector**

In addition to the work of the private certification bodies, important security certification activities take place in the public sector. The database of the DAkkS lists for example 23 accredited police organisations in the security field.

Besides standards, internal guidelines with restricted access are used, for example documents on ‘Specific Operation Procedures’ (SOPs) for inspection (e.g. for voice analyses), Arbeitsanweisungen (AA) of the BKA as well as BKA documents for IT forensic. The Beschussamt Ulm Staatliche Prüf- und Zertifizierungsstelle für Waffen- und Sicherheitstechnik is another interesting player, which even uses NIJ standards from the
In the following sections we will provide insight in two areas: aviation security/air cargo and IT security.

Aviation security/air cargo

Aviation security is shaped by a complex landscape of responsibilities in Germany. The key players, which are on top of the relevant hierarchy in Figure 31, are the Federal Ministry of Transport and Digital Infrastructure (BMVI) and the Federal Ministry of the Interior (Bundesministerium des Innern, BMI). On the next level are the federal authorities (the ‘Landesbehörden’), the Federal Police and the Federal Aviation Authority (‘Luftfahrt-Bundesamt’, LBA).

The BMI is the highest authority regarding passenger checks, baggage checks and tests of the reliability of the staff while the BMVI is the highest authority of cargo scanning and the security requirements for airlines. In addition, the BMVI represents Germany in European negotiations regarding aviation security in Brussels. The federal authorities are mainly responsible for the security measures at airports and for the security checks of airport staff. In addition, they are responsible for passenger checks and baggage checks at several airports.

The LBA is responsible for controlling the aircraft, safeguarding of the airlines and the flight agents. Based on regulation EC 2320/2002\textsuperscript{233} the 36 civil German airports are subject of specific security measures. The Federal Police is responsible for the security of 14 mainly large

\textsuperscript{231} More information on the NIJ will be given in the country study “United States”


airports while the federal authorities are responsible for the remaining 22, mostly small airports. In total, there are 20 authorities involved in aviation security in Germany: 16 federal authorities, the Federal Police, the LBA, the BMI and the BMVI.

Each airport and each airline has to submit an aviation security plan to its competent authority. The federal authorities are responsible for the airports and the LBA is responsible for the airlines. In addition, Germany had to develop a national quality control programme, which means that each month one of Germany’s 36 airports is subject to an audit. This means also that each airport is audited every 36 months or every three years. The audit teams consist of representatives of the competent authorities: one of the federal state, one of the LBA, on of the federal police and sometimes one of the BMVI or the BMI. Each audit lasts for one week. In addition, the European Commission also sends teams of inspectors into the Member States and supervises the implementation of security measures – not only at the airports but also at the authorities of the Member States. In this context, the tasks of the Bundespolizei (Federal Police) include:

- Testing of police and control equipment
- Testing of control processes
- Responsibility for European and national admission tests for police and aviation security equipment
- Participation at European committees for standardisation and certification
- Lays out requirements for tenders
- Single approval for control equipment at airports
- Simulates and analyses control processes
- Coordinates the police R&D on security.

The responsible unit is the Forschungs- und Erprobungsstelle der Bundespolizei. The Bundespolizei also belongs to Europe’s five providers of European Civil Aviation Conference (ECAC) tests. The testing is done in close collaboration with a laboratory of the Fraunhofer Institute für Chemische Industrie (ICT). The Test Center for Explosives Detection Systems operates on behalf of the German Federal Police. With regard to CRISP, two services of the test center for Explosives Detection Systems are relevant: the ECAC certification test and the ICT Test.

**ECAC certification test**

The official ECAC certification test covers the following explosives detection systems:

- Metal detectors
- Detection systems for checked baggage
- Detection systems for hand luggage
- Security scanners
- Trace detection systems.

The application from the manufacturer is made under the framework of the ECAC’s “common evaluation process” (ECAC-CEP) in the ECAC office. The system developers receive a lim-

---

ited feedback after the final meeting. The results of the performance analysis are passed on to the ECAC within classified reports. Systems, which have not achieved the defined performance standard, can retake the certification test after system development or, in some specific cases, can take a so-called “simulated retest” (SRT) on basis of a raw data set from an experimental testing series.\footnote{Fraunhofer ICT, “ECAC certification test”, no date.}

**ICT Test**

The ICT test includes a tailored testing procedure. Depending on the type of system, the manufacturer can choose between a multitude of solid, liquid or traces of explosives from the commercial or military sectors, as well as so-called ‘home made’ explosives. A representative luggage set is also available, with which the detection of explosives in hand luggage can be simulated. Besides measuring the detection performance for actual explosives, the false alarm rate can be determined using so-called ‘benign sets’ comprising 500 samples such as cans, care products, spirits etc. A detailed test report is created and the raw dataset is made available to the client.\footnote{Fraunhofer ICT, “ICT test”, no date.}

**Excursus: civil drones**

A specific issue, which CRISP has selected in particular for its work packages 3 and 4, is the certification of civil drones. In Germany,\footnote{This section builds on conversation with a member of a German public authority.} only the use of light drones up to 25 kilograms is allowed. The framework conditions are specified by the Luftverkehrsordnung, in particular §§ 15 and 16. In addition, a ‘Musterzulassung’ plus several safety regulations exist. Video drones are regarded as model aircrafts. Federal authorities of the German ‘Bundesländer’ are responsible for their admission. Commercial use of such systems is embedded in specific framework conditions.

**IT security and cryptography**

Based on the law BSI-Errichtungsgesetz, the Bundesamt für Sicherheit in der Informationstechnik (BSI) has the duty to issue security certificates for products, systems and components of information technology. The BSI, which is accredited by the DAkkS, works together with the following institutions:

<table>
<thead>
<tr>
<th>Name of test center</th>
<th>Area of assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>atsec information security GmbH</td>
<td>Common Criteria (CC)\footnote{Fraunhofer ICT, “ECAC certification test”, no date.}</td>
</tr>
<tr>
<td>brightsight bv</td>
<td>CC + SC*</td>
</tr>
<tr>
<td>datenschutz cert GmbH\footnote{Fraunhofer ICT, “ICT test”, no date.}</td>
<td>CC</td>
</tr>
<tr>
<td>Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) GmbH</td>
<td>CC</td>
</tr>
</tbody>
</table>

\footnote{More information on CC will be given in the chapter on international certification schemes.}

\footnote{More information will be given in chapter 3.4.5.2.}
So far, the BSI has signed the CCRA Agreement for the European approval of IT security certificates and the SOGIS-MRA for worldwide approval. BSI certificates are granted for solutions, which are in line with public interest - especially security interests of the Federal Republic of Germany (BSIG § 9 (4) 2. As a result, the approval is limited in terms of

- The selection of cryptographic algorithms and functions and
- Test results for the implementation and the strengthening of cryptographic algorithms and functions.

In these areas, national rules and regulations take precedence. BSI’s certificates have an excellent image not only in Germany but also in Europe and worldwide. Therefore many foreign companies come to Germany and seek to receive such a certificate.

**Current work**

In January 2011, the workshop ‘certification of security technologies and services’ took place in Berlin at the DIN Deutsches Institut für Normung. Around 100 people from government, industry, academia and associations attended the event. Four priorities for action were defined:

- European Security Label
- Harmonisation of minimum requirements for the private operation of critical infrastructures (e.g. energy networks)
- Certification of system integration (management / systems / processes)
- Certification of services (service, education, training).

As shown in the list, certification is considered as appropriate for products, systems and processes. The structuring of certification programs should build on existing structures. According to the press release of the conference, a certification system with three layers was suggested with

- The certification of management systems (e.g. ISO 9000) on top,
- Industry-related system certifications (e.g. ISO 27001, ISO 28000) on the second level and
- The certification of products and services on the third level.

Infrastructures, processes, people and information have been identified as core topics. The following figure summarises the ideas.
Security services on the other hand are far more heterogeneous than technologies and products, which led to the recommendation of a sectoral approach. Therefore the certification focus should be on processes and training. Major topics for security services are crisis management, handling of incidents, securing infrastructure and Business Continuity Management (see also CRISP Deliverable 2.1).

3.4.5. SELECTED SECURITY CERTIFICATION BODIES AND THEIR WORK

3.4.5.1. EXTENDED EXAMPLES

This sub-chapter describes the services of five certification bodies (VdS, ECB, BHE, TÜV/TÜV Rheinland and datenschutz cert) in detail. The selection was based on the aim to provide information on the certification of specific security solutions, e.g. in the fields of CCTV systems and security services. In addition, a mix of certification fields (products, systems, persons etc.) was sought. Many international certification bodies come from Germany and analysing each organisation is not possible. In addition, there are European countries, in which security-related certification services are mainly offered by the subsidiaries of German certification bodies, e.g. TÜV Süd and TÜV Nord and their services could be analysed by other national CRISP partners. Therefore the main focus in this country study was on specific national players in Germany.

VdS Schadensverhütung

VdS is an independent institution and certification body, which aims to ensure safety and trust in the fields of fire protection and security. It develops advanced safety and security concepts for industrial and commercial enterprises, manufacturers and system businesses as well as specialist firms and independent specialists. VdS is accredited in many areas including the certification of products based on DIN EN ISO/IEC 17025, of management systems based on DIN EN ISO/IEC 17021 and different security and safety services based on DIN EN 45011.
It is also a “Type A” inspection body for fixed fire protection systems based on DIN EN ISO/IEC 17020.\textsuperscript{241} Its services in the security field have the following characteristics:

### Kinds of PSS which are tested and certified in the security field

Solutions for fire protection and security in general; service providers, security services providers (e.g. installation companies), alarm receiving centers; security containers, electronic security solutions, software applications, fire-extinguishing systems

### Certification process(es) in the security area

A market player (e.g. a manufacturer) decides to commission VdS based on a specific guideline

1. **Test:** is the certification of the solution possible?
2. Development of a test plan
3. Testing procedure
4. Evaluation: requirements vs. fulfilment
5. Formal decision to grant a certificate or not based on the results
6. Issuing the certificate which shows the field of application and the period of validity:
   - software: 3 years, hardware: 4 years, services: 1 year
7. Validation after the period of validity
   - e.g. intruder detection systems: evaluation in the present setting every fourth year

Example: fire protection – the certification process is defined by standard DIN 14675

### Documents which form the basis of the testing and certification process(es)

- **Standards:** European and German standards for testing and certification
- **Laws/regulations:** yes, if applicable, e.g. an European directive for Fire Safety
- **Documents from Deutsches Institut für Bautechnik; Brandschutzordnung**
- **Internal guidelines and additional documents**
  - VdS Richtlinien (whose development is often initiated by insurance agencies)
    - Context: European standards reflect the minimum consensus in the Member States. The Richtlinien describe additional requirements, e.g. to overcome the problem that no European standard for software in security and safety products exists. They are also used to specify requirements on CCTV cameras based on EN standards from CLC TC 79.
    - Examples of VdS Richtlinien:
      - VdS 2364 VdS-Richtlinien für Videoüberwachungsanlagen. Systemanforderungen. Kategorie I
      - VdS 2365 VdS-Richtlinien für Videoüberwachungsanlagen. Systemanforderungen. Anforderungen an Videoüberwachungssysteme der Kategorie II
      - VdS 3112en Biometric recognition procedures Requirements and Test Methods

### Prüfvereinbarungen

Prüfvereinbarungen are used for the testing of innovative technologies, which are not addressed by a standard so far. The foundation for the testing process is a contract, which defines the testing criteria. The criteria are specifically defined for the new technology field.

D2.2: Consolidated report on security standards and certification

CRISP project

<table>
<thead>
<tr>
<th>Security PSS which are certified based on the aforementioned standards</th>
<th>Standard(s) used in the certification process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smoke alarm devices for home use</td>
<td>DIN 14676</td>
</tr>
<tr>
<td>Security containers</td>
<td>EN 1300, VdS 2396</td>
</tr>
<tr>
<td>Biometric recognition procedures</td>
<td>VdS 3112en</td>
</tr>
<tr>
<td>Intruder detection system</td>
<td>EN 50131 or VdS guidelines, depending on the mentality of the manufacturer and the geographical target market. Example: the Spanish market requires conformity to EN standards, not to VdS guidelines while the markets in Germany and outside Europe prefer the VdS certification. An alternative to the different solutions is offered by EN 50131. It provides several amendments according to national preferences.</td>
</tr>
</tbody>
</table>

| Fields which are addressed by EN 54 | EN 54 (the series of European standards for voice alarm products and parts of the European Union's Construction Products Directive. The use of EN 54 certified products for all new voice alarm installations became mandatory in April 2011.242) |

<table>
<thead>
<tr>
<th>Security PSS which are certified based on any other aforementioned documents (laws/regulation, internal guidelines/documents etc.)</th>
<th>Document(s) used in the certification process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product/technology/system/service</td>
<td>VdS documents</td>
</tr>
</tbody>
</table>

| Quality seal |
| --- | --- |
| ![VdS seal](sourceen54.eu) |

Key evaluation criteria in the security field and requirements for obtaining a certificate - examples

<table>
<thead>
<tr>
<th>Product/technology/system/service: intruder detection product e.g. with infrared</th>
<th>Evaluation criterion</th>
<th>Minimum requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality, sabotage security, electromagnetic compatibility, operational safety, air stability, usability, user manual standards: time, distance</td>
<td>VdS guidelines (based on specific intrusion scenarios): identification of a wrong resolution of infrared and of missing resolutions</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product/technology/system/service: fire detectors</th>
<th>Evaluation criterion</th>
<th>Minimum requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Someone is trying to put fire</td>
<td>Specific parts of the EN 54 series</td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Product/technology/system/service: security container on a specific security level</th>
<th>Evaluation criterion</th>
<th>Minimum requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destruction test based on a scenario with a particular time and particular tools</td>
<td>according to the relevant standard</td>
<td></td>
</tr>
</tbody>
</table>


**VdS 2364**
Basic requirements, e.g. DIN EN 50130-4 regarding electromagnetic compatibility, DIN EN 50130-5 regarding environmental audits; Specific requirements: compatibility, specific requirements regarding image generation, image transmission and image presentation, storage, export of data, system security, ability to detect disruption of system components, protection against tempering, secure transmission of image data, access to the system and related measures, energy supply, operational safety, functional safety

**VdS 2365**
Protection against environmental influences, functional safety, operational safety, existence of measures for access authorisation (e.g. finger print, password etc.), protection against tempering, energy supply, interfaces; data protection issues are considered as follows (translation): “In the evaluation of the recorded data, it may be necessary for privacy reasons that access to such data may be only possible by two people (four eyes principle). For this reason, video recording devices should offer the possibility to get access to the specific access level 2 via two passwords only.”

Conformity assessment is based on a specific test assembly, which is described and visualized in both guidelines

**Cooperation with external test laboratories in the security field**
in exceptional cases (for example with the ‘Verband der Schloss- und Schlüsselindustrie,’ BAM\(^{243}\) regarding explosives testing, EFSG and other laboratories)

**Involvement of the organisation in security standardisation**
Yes, like in the German mirror committee of CEN/CLC TC 4 as well as in all relevant committees at DKE and DIN; CLC TC 79, TC 79/WG 7 Video Surveillance; development of EN 50131 and of standards for transmission technology

**Number of certificates issued in the security field annually**
4,000 including re-certification, approx. 25% new certificates
The number depends on the activities in the standardisation landscape, in year 2014 32 standards, which are relevant for the activities at VdS, were modified

**(Mutual recognition) agreements with other EU countries/CABs in the security field**
Yes, based on the participation in the EFSG, further activities include: intense exchange of experiences, e.g. regarding the interpretation of standards, tests etc.

\(^{243}\) Bundesanstalt für Materialforschung und -prüfung
Solutions for suppliers of certified security solutions from other European countries that wish to receive a certificate that is valid in the country

VdS offers suppliers from a number of EU countries mutual recognition. In addition, market observation is used to find appropriate solutions.

Example of mutual recognition: A manufacturer wants to receive a certificate, which is relevant in Germany and France. He contacts one of the two national EFSG partners, both decide together who will conduct the test. The other institution receives the results and may add additional tests according to additional national requirements.

VdS is accredited based on EN ISO/IEC 17065 and this standard forbids that owners of a certificate from a foreign EFSG partner seeks recognition in Germany later. EFSG aims to agree beforehand on the test design and the test report. The involvement of other certification bodies is to determine in advance.

Companies from countries without EFSG partners can commission VdS to carry out a certification process, which enables them to receive a valid certificate for Germany. Previous certificates are evaluated individually.

Obstacles regarding the enlargement of the EFSG network and the inclusion of new members include:

- Failure of candidates to demonstrate the required experience
- Lack of willingness by candidates to participate in EFSG’s quality management measures including the use of the EFSG auditing system, multilateral supervision and round robin tests
- Necessary efforts to participate (time for negotiations) etc.

Summary

VdS is an important player in Germany and collaborates actively on a European level. According to the DAkkS database, VdS is the only certification body in Germany, which is accredited for the certification of video surveillance systems (in German ‘Videoüberwachung’). VdS 2365 provides an interesting example of how to deal with privacy issues in the certification process.

ECB

The European Certification Body (ECB) is a neutral certification body accredited to EN ISO/IEC 17065. At present, there are approximately 1,000 valid ECB-S certificates in the global security market. ECB has more than 40 years of experience in the testing and certification of security technology.244

Kinds of PSS which are tested and certified in the security field

| Burglary resistance products: Secure safe cabinets, safes, ATM safes, ATM bases, strongroom doors, strongroom walls, deposit systems and high security locks |
| Fire resistance products: light fire storage cabinets, data cabinets (security systems), diskette inserts, data rooms and data containers |
| Burglar resistant construction products: burglar resistant doors, burglar resistant windows, bullet resistant doors and bullet resistant windows. Furthermore ECB-S product certifications are being prepared for fire safety storage cabinets, building hardware and apertures of private letter boxes and letter plates |

244 ECB, “The ECB – Competence in certification matters”, no date. http://www.ecb-s.com/_rubric/index.php?rubric=ECB-S+EN+Certification-body, the following table builds on an interview and information given on ECB’s website
Certification process(es) in the security area

The certification procedure of ECB is based on three parts. They aim to ensure that the certified product characteristics are in accordance with the relevant European standards. The certification procedure comprises: type test, certification and external quality surveillance. The type test carried out at the recognised laboratories of ECB and the certification are exclusively based on the requirements of the relevant European standard. Additional requirements do not exist. Each certificate is valid for four years. In accordance with its certification guidelines, ECB carries out periodical external quality surveillance audits at the manufacturing plants. During these visits it is ascertained whether the production is based on the approved technical documentation. In addition, the auditor ascertains whether the manufacturer uses a certified quality management system according to ISO 9001/EN ISO 9001.

Documents which form the basis of the testing and certification process(es)

<table>
<thead>
<tr>
<th>EU Documents</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN 1143-1</td>
<td>Safes, ATM safes, strongroom doors and strongrooms</td>
</tr>
<tr>
<td>EN 1143-2</td>
<td>Deposit systems</td>
</tr>
<tr>
<td>EN 14450</td>
<td>Secure safe cabinets</td>
</tr>
<tr>
<td>EN 1047-1</td>
<td>Data cabinets and diskette inserts</td>
</tr>
<tr>
<td>EN 1047-2</td>
<td>Data rooms and data containers</td>
</tr>
<tr>
<td>EN 1300</td>
<td>High security locks</td>
</tr>
<tr>
<td>EN 15659</td>
<td>Light fire storage units</td>
</tr>
<tr>
<td>EN 1627</td>
<td>Pedestrian doorsets, windows, curtain walling, grilles and shutters - Burglar Resistance - Requirements and classification</td>
</tr>
<tr>
<td>Other</td>
<td>The recognised high security locks for installation in ECB•S-certified secure storage units are documented in the Lock Guide ECB•S R01.</td>
</tr>
</tbody>
</table>

Quality seal

The ECB•S certification mark documents that the security products have been certified by ECB, meet the requirements of the relevant European Standard and have been manufactured under a certified quality management system according to ISO 9001 (EN ISO 9001).

The certification mark shows the ECB•S serial number by which the manufacturer can be identified. It clearly defines the performance range of the product: security level, resistance grade, protection class, lock class and resistance class.

Key evaluation criteria and requirements for obtaining a certificate - examples

- High security locks: according to the relevant EN standard, Sweden has additional requirements, which could be included in the standard
- Data rooms: according to the relevant EN standard, ECB is the only accredited CAB in this field
- Burglar resistant products: the EN specifies the tools for the test but there is also the human factor (the EN does not specify the burglary test itself) - ECB ensures that the qualification of the testers is comparable in the different laboratories
### Cooperation with external test laboratories in the security field

ECB collaborates with a number of laboratories across Europe. It is a specific characteristic of ECB that customers can select a laboratory based on this list according to their wish.

### Involvement of the organisation in security standardisation

ECB’s involvement includes almost all areas in which the company is active. It holds the secretary of CEN TC 263 Secure storage of cash, valuables and data media, WG 1 Burglary resistance and WG 2 Fire resistance and will also hold the secretary of WG 3 High Security Locks in the near future.

### Number of certificates issued in the security field annually

Around 400

### (Mutual recognition) agreements with other European countries/certification bodies in the security field

ECB belongs to EFSG, the European Fire and Security Group, which has also members in France, Sweden, Denmark and the United Kingdom. EFSG’s agreements cover the fields of High Security Locks, safes and strongrooms.

### Solutions for suppliers of certified security solutions from other European countries that wish to receive a certificate that is valid in the country

ECB accepts tests of laboratories which belong to its network. Theoretically, suppliers with other tests need a new test but it is possible that ECB contacts the relevant laboratory and suggests conducting common tests to compare the results afterwards. Such processes are time-consuming.

### Summary

ECB has a European character and shows good practice in several fields. Only European standards are used for certification, no national standards and no additional guidelines. The customers can choose between several test laboratories in different countries. ECB is internationally recognised. Around 20% of the customers are even non-Europeans. Most products and other solutions addressed by ECB’s services do not include the use of data. This absence of potential ethical risks avoids the need for specific additional tests. ECB also provides detailed information on the certified products on its website, which allows appropriate comparisons.

### BHE Bundesverband Sicherheitstechnik e.V.

The BHE Bundesverband Sicherheitstechnik e.V. is a major German Association for security and safety technology and has currently nearly 800 member companies, including approx. 78% installers, 20% manufacturers and 2% planners. Among other tasks, BHE offers its members security certification services to gain two kinds of certificates: certificates for installers (BHE-certified specialist) and certificates for planners (BHE-certified planners). Since the introduction of the seal about 30 years ago, more than 1,000 certificates have been issued so far. Although the indented key benefit of the certificate is to strengthen the relationship
between installers and customers, BHE notices an increasingly positive acceptance by insurers, criminal counseling centers and fire departments etc.245

<table>
<thead>
<tr>
<th>Kinds of PSS which are tested and certified in the security field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Companies / services in the following fields: fire alarm systems, intrusion alarm systems, open-air surveillance systems, mechanical safety systems, smoke and heat exhaust ventilation systems, voice alarm systems, video surveillance systems, access control systems</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Certification process(es) in the security area</th>
</tr>
</thead>
<tbody>
<tr>
<td>The steps of awarding the certificate can be described as follows:</td>
</tr>
<tr>
<td>• The responsible specialist completes a test (Fachkundeprüfung) at BHE</td>
</tr>
<tr>
<td>• After successfully passing the evaluation of the application documents, the BHE gives the applicant the certificate</td>
</tr>
<tr>
<td>• If the applicant has already passed a comparable test at another institution, which is accepted by the BHE, e.g. from the VdS, the certificate is recognised</td>
</tr>
<tr>
<td>• Regularly over time (at least once in two years) the responsible specialist must participate in a training course in the relevant field of security technology</td>
</tr>
<tr>
<td>• The resign of a company's chief operating specialist must be notified immediately to the BHE. For a transitional period of six months, a new chief responsible specialist has to be appointed.246</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Documents which form the basis of the testing and certification process(es)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standards</strong></td>
</tr>
<tr>
<td><strong>Laws/regulations</strong></td>
</tr>
<tr>
<td><strong>Internal guidelines/documents</strong></td>
</tr>
<tr>
<td><strong>Other documents</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security PSS which are certified based on the aforementioned standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>See ‘Kinds of PSS, which are tested and certified in the security field’</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security PSS which are certified based on any other aforementioned documents (laws/regulation, internal guidelines/documents etc.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>See above, they are certified based on the guidelines, which build on national, European and international standards</td>
</tr>
</tbody>
</table>

Quality seals

Example perimeter/outdoor detection

The seal ‘BHE-certified specialist for outdoor detection systems’ confirms that the certified provider plans, installs and maintains outdoor detection systems in compliance with the relevant standards and regulations. The BHE-certified specialist

- knows the rules and the object and provides customized solutions
- is available day and night to ensure the functioning of the system
- has service quantities always in stock
- ensures that the complex test instruments and tools for the proper functioning of the plant are always available
- ensures that his service technicians are regularly trained and educated
- has all the technical requirements and resources to perform the required work efficiently and in the best quality.

---

**Key evaluation criteria in the security field and requirements for obtaining a certificate**

<table>
<thead>
<tr>
<th>Internal test</th>
</tr>
</thead>
</table>

**Cooperation with external test laboratories in the security field**

| Not applicable |

**Involvement of the organisation in security standardisation**

| BHE represents member companies in national and international standardisation |

**Number of certificates issued in the security field annually**

| More than 1,000 certificates have been issued so far |

**Mutual recognition) agreements with other European countries/certification bodies in the security field**

| Agreement with the German certification body VdS, no agreements with foreign CABs |

**Solutions for suppliers of certified security solutions from other European countries that wish to receive a certificate that is valid in the country**

| They can apply for a certificate, other certificates are not recognised. |

**Summary**

BHE offers its members the opportunity to apply for a certificate for low cost:

- Awarding the certificate for companies, which have already comparable certificates (e.g. VdS, DIN 14675): free of charge
- Awarding the certificate for companies without comparable admission: € 130 + Tax.
- Awarding the certificate for subsidiaries: per subsidiary € 30.00 + tax
According to BHE, the good price is also based on the fact that this organisation does not invest in accreditation. Many small companies belong to BHE’s target group. According to BHE the seal enjoys strong acceptance in the market, the demand site of the market requires security systems with a BHE certificate.

TÜVs (Technische Überwachungs-Vereine)

The TÜVs (Technische Überwachungs-Vereine) are well known industrial certification bodies. Originally local organisations, they have merged into five large groups with regional names but international activities: TÜV SÜD, TÜV Nord, TÜV Rheinland, SG TÜV Saarland as well as TÜV Austria in the neighbour country Austria.

TÜV SÜD offers a wide range of services in the field of infrastructure security including testing and certification of bridges and engineering structures, security systems, alarm receiving centres as well as penetration testing of communications systems. TÜV Nord lists certification services in the road, rail, health, food and feed, aviation and oil and gas sectors, including for explosion-protected equipment and machinery. TÜV Rheinland provides for example certification of industrial plant and pressure equipment and explosives products. It is described in more detail below. TÜV Austria was already described in the Austrian chapter.

TÜV Rheinland and the establishment of ARGE DIN 14675

ARGE DIN 14675 is an association of currently ten accredited certification bodies and the owner of an accredited certification scheme for the planning, operating and maintenance of fire alarm systems and voice alarm systems based on the DIN standard on ‘Fire detection and fire alarm systems - Design and operation’. It is in the first place a voluntary arrangement of both certification bodies and interested parties. Interested parties are the manufacturers, planners and constructors of evacuation and fire alarms. It is aimed at all certification bodies, which offer certification according to DIN 14675 (various fire alarm systems) but is not limited to them.

The goal of ARGE DIN 14675 is to ensure a minimal quality level for all DIN 14675 products. It also aims to secure the high quality level, based on the existing laws and standards and to further develop the certification scheme. In accordance with those goals, the ARGE DIN 14675 has laid out regulations for the examination process of the responsible workers, for the questionnaires and in case of fire alarms also the additional project planning examination for the fire alarm departments.

The DIN ARGE is represented by the Verband akkreditierter Zertifizierungsgesellschaften e.V. with a new spokesperson (and a deputy) being elected every 24 months. The spokesperson does not only represent the DIN ARGE 14675 to the outside world. He/she is also responsible for part of the internal organisation, for examples of meetings, which the members should attend.

---

Membership is voluntary and free of charge. The current members, listed on the webpage and dated of 2012 are: VdS Schadenverhütung GmbH; TÜV Industrie Service GmbH; TÜV Rheinland Group; TÜV Nord CERT GmbH & Co. KG; DQS GmbH; TÜV Technische Überwachung Hessen GmbH; LGA InterCert Zertifizierungsgesellschaft GmbH; TÜV SÜD Industrie Service GmbH; TÜV Thüringen e.V. and the ZDH-Zert GmbH. New members are welcome and will be admitted upon having sent a written application for membership. There are no clearly stated requirements for membership. This membership can be canceled at any time through again a written statement.

Representatives of interested parties are welcome and have the same participation rights as the members and should be given opportunity to participate. They receive invitations and relevant documents at the same time as the members. The obligations of the members include keeping the agreed guidelines, using the specific assessment catalogs, actively cooperating in the ARGE and involvement in the further development of the scheme. The guidelines and assessment catalogs are online available for free. External certification bodies, which wish to use these guidelines or the assessment catalog, have to seek permission by the ARGE. The guidelines are checked annually for accuracy and applicability, especially regarding new or changed framework conditions or relevant standards. They were initially published in 2004. The second edition was published in 2006, the third in 2009 and the current one in 2012. These current certification requirements have been acknowledged and approved by the DAkkS (the earlier versions were certified by the previous accreditation body).

As an example of the cooperation, the ARGE’s working group responsible for its examination questions, has more participants than the members listed above as interested parties are also included. These also include the Bundesverband der Hersteller- und Errichterfirmen von Sicherheitssystemen (BHE) e.V. and the Zentralverband Elektrotechnik- und Elektronikindustrie e.V. (ZVEI), which are important industry associations in Germany.

**Datenschutz cert GmbH**

The datenschutz cert GmbH is a company of the datenschutz nord Group. It offers conformity assessments in the field of data protection and information security, which include both testing and certification activities. The focus is on IT systems, products, procedures and processes. According to its website, datenschutz cert is accredited by eight institutions. The following lists shows the relevant bodies and certification services/certificates:

- Deutsche Akkreditierungsstelle (DAkkS): certification body for ETSI TS, ISO/IEC 20000-1 and ISO/IEC 27001
- Bundesamt für Sicherheit in der Informationstechnik (BSI):
  - Auditteamleiter according to ISO 27001 auf der Basis von IT-Grundschutz
  - IS-Revisoren
  - IT-Sicherheitsdienstleister für IS-Revision und IS-Beratung
  - Prüfstelle für IT-Sicherheit für Common Criteria
  - Prüfstelle für IT-Sicherheit für TR-ESOR
- Bundesnetzagentur

---

Bestätigungsstelle für Produkte gemäß Signaturgesetz
- Prüf- und Bestätigungsstelle für Sicherheitskonzepte gemäß Signaturgesetz

- Initiative D21: ips-Datenschutz-Zertifikat
- EuroPriSe GmbH: Gutachter für die Bereiche Recht und Technik gem. EuroPriSe (more information on EuroPriSe is given in chapter 6)
- Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein: Prüfstelle für die Bereiche Recht und Technik gem. DSGSVO-Datenschutz-Gütesiegel

Datenschutz cert provides eight data protection seals in the following fields:

- Auftragsdatenverarbeitung - Zertifizierung von Auftragsdatenverarbeitern gemäß § 11 BDSG
- bevh-Datenschutzgütesiegel - Prüfung und Zertifizierung von Unternehmen im E-Commerce und Versandhandel gemäß bevh-Datenschutzgütesiegel
- Bremisches Datenschutz-Gütesiegel - Prüfung von Verfahren und technischen Einrichtungen zur Erlangung des Datenschutz-Gütesiegels gemäß Bremischer Datenschutzauditverordnung (BremDSAVO)
- Datenschutz-Zertifikat - Prüfung und Zertifizierung von Datenschutzmanagement-systemen
- EuroPriSe Datenschutz-Gütesiegel - Prüfung von Produkten und Verfahren zur Erlangung des Europäischen-Datenschutz-Gütesiegels (European Privacy Seal, information is given in chapter 6)
- ips - internet privacy standards - Prüfung und Zertifizierung von Webseiten gemäß Datenschutz-Gütesiegel ips internet privacy standards
- ULD-Datenschutz-Gütesiegel - Prüfung von Produkten zur Erlangung des Datenschutz-Gütesiegels des ULD (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein)
- Zertifizierte Datenschutzbeauftragte - Prüfung und Zertifizierung von betrieblichen Datenschutzbeauftragten (bDSB) als Fachkundenachweis

The following figure shows all seals in these areas:

Source: Datenschutz cert GmbH (own and external seals)
Figure 34: Data protection seals available at the datenschutz cert GmbH

In addition, datenschutz cert provides 21 different certificates for the specific fields of IT security. More information is provided at: https://www.datenschutz-cert.de/leistungen/nach-thema/it-sicherheit.html

3.4.5.2. BRIEFLY DESCRIBED EXAMPLES

This section briefly describes the activities of four other important certification bodies in the security field, DEKRA, DNV and SGS.

DEKRA

DEKRA is one of the world’s leading providers of expert services. Its Annual report 2013 illustrates the following performance data: more than 25,000 system certifications and more than 23,000,000 vehicle inspections. An important service in the security field is related to air cargo. DEKRA Cargo & Security Services Ltd. conducts air cargo inspections on behalf of the customer, which guarantee compliance with all security and safety requirements of air cargo.253 DEKRA also gives advice on the admission as a ‘reglemented’ agent, known consignor and ‘reglemented’ supplier, on the creation of aviation security plans and programmes, the introduction of a safety management system as well as on the obtaining of the certificate AEO – ‘Authorized Economic Operator’.254 Further information is available at www.dekra-aviation.de.

DNV

DNV is a world leader in many technical service and consulting areas related to sea transport and energy and is also one of the top three certification bodies in the world. In the security field its certification based on the International Ship and Port Facility Security (ISPS) Code is important. According to the code, stakeholders (governments, shipping companies, crew and port or facility staff) have to certify security of the following ships engaged in international voyages:

- Passenger ships, including high-speed passenger craft
- Cargo ships, including high-speed craft, of 500 gross tonnes and upwards
- Mobile (self-propelled) offshore drilling units255

For ships over 500 GT in international trade, ISPS certification is mandatory. Local DNV GL offices offer ISPS services at over 300 sites in more than 100 countries. The services include:

- An approved Ship Security Plan (SSP) and a full-term International Ship Security Certificate (ISSC) for individual ships to fulfil mandatory security requirements stated by the IMO through the ISPS Code

253 Background: At the end of a transitional period, all air freight shipments are considered unsafe if they do not come from exporters that the Federal Aviation Authority had certified as a known consignor in accordance with Regulation (EC) No 300/2008 and Regulation (EC) No 185/2010. After that period, insecure cargo must always be checked before air transport, see chapter 1.2.
- Review of the SSP and approval of the SSP
- Interim Shipboard Verification
- Issuance of an interim International Ship Security Certificate (ISSC) that is valid for six months
- Initial Shipboard Verification done during the interim period
- Issuance of a full-term ISSC that is valid for five years
- In the process of ISPS certification, audits that are combined with the ship’s International Safety Management (ISM) certification may be carried out in order to save the customers time and money.

DNV offers several tools and guidelines for preparing and performing a Ship Security Assessment (SSA), which is then needed to create a Ship Security Plan (SSP). The SSP is then approved by DNV GL as Recognised Security Organisation (RSO) on behalf of the flag administration. To implement the SSP onboard, an interim audit is done and an interim International Ship Security Certificate (ISSC) is issued, valid for six months. Based on the successful completion of an initial or renewal audit, an ISSC is issued and valid for five years. An intermediate audit is carried out two years after the relevant audit.\footnote{256 DNVGL, op cit., no date.}

**SGS**

SGS is a world leader for inspection, verification, testing and certification. Amongst the many certification services that they offer, relevant to this report are: certification of scanners used for border security, certification of tanks, pressure vessels and wind energy projects, waste water systems certification and certification of business continuity, risk management and financial systems. They are a notified body for almost all EU product safety directives.\footnote{257 Lewis, op. cit., 2014} In addition, SGS provides, for example, audits based on the Customs-Trade Partnership Against Terrorism (C-TPAT). C-TPAT was introduced by the U.S. Customs Service in 2001 and is a voluntary safety programme for the supply chain. It aims at improving the security of the supply chains of companies and has more than 9,000 partners.

SGS provides a security audit tool for supply chains, which builds on C-TPAT’s security requirements and aims to ensure compliance with C-TPAT rules at each stage of the supply chain. Based on regular audits, SGS continuously monitors their customers’ compliance with C-TPAT. In addition, it offers assessments of the conformity of the safety systems and procedures of current or potential third-party manufacturers under contract, freight forwarders and similar service providers based on a risk assessment of the entire supply chain.

The C-TPAT audit process of SGS usually consists of four steps:

1. Based on its checklist and criteria, an audit programme related to the customer’s needs is created
2. The auditors conduct on-site audits of the customer’s locations
3. After the completion of the audit, SGS provides the customer with a full audit report. This report is checked again by its technical experts before it is sent to relevant parties

---

\footnote{256 DNVGL, op cit., no date.} 
\footnote{257 Lewis, op. cit., 2014}
of the contract. At this time, SGS makes also recommendations for future improvements.

4. SGS continues monitoring according to the contract that the customer complies with C-TPAT.

The TAPA certification of SGS provides an examination of all safety-relevant elements in the customer’s organisation, including employee checks, perimeter security, burglar alarm systems, surveillance systems, value storage and transit delays. During the audit itself, all warehouses and distribution centers of the customer are investigated regarding security-related issues. The customers also receive support in the definition of requirements for minimum driver safety.\(^{258}\)

SGS-TÜV Saarland also certifies machinery, buildings, pressure equipment, water systems and staff, and IT security according to ISO 27001 and the BSI Grundschutz\(^ {259}\).

**Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. and Datenschutz Zertifizierungsgesellschaft mbH (DSZ)**

The Association for Data Protection and Data Security (GDD) is a non-profit organisation for practicable and effective data protection. It interacts with government officials, data protection authorities, associations and privacy experts.

Building on German data protection law (BDSG), GDD developed the data protection 'standard' DS-BvD-GDD-01 for service providers, Datenschutz Zertifizierungsgesellschaft mbH (DSZ) offers certification based on this standard.\(^ {260}\)

### 3.4.6. **ADDITIONAL SOLUTIONS**

Interesting examples for the evaluation of security solutions are not only provided by certification bodies, test centers and specific EU projects (e.g., CREATIF\(^ {261}\)). The development of evaluation methods is often also a sub-task of technical research projects to allow for self-assessment of project results and to provide external parties with opportunities to determine the technical success of these projects.

Regarding one of CRISP’s core interests in CCTV, an expert mentioned that several projects funded by the Federal Ministry of Education and Research (BMBF) also included the development of interesting evaluation methodologies. Based on this information, an additional expert, who deals with national security projects, was contacted. According to this source, selected results of three projects in particular are relevant:

---


\(^{259}\) Lewis, op. cit., 2014


\(^{261}\) More information on CREATIF and similar projects is provided in chapter 6.
D2.2: Consolidated report on security standards and certification

- CamInSens - Verteilte vernetzte Kamerasysteme zur in situ-Erkennung Personen-induzierter Gefahrensituationen,\(^{262}\)
- ASEV Automatische Situationseinschätzung für ereignisgesteuerte Videoüberwachung (ASEV)\(^{263}\) as well as
- MOVIT Mustererkennung und Video Tracking: sozial-psychologische, soziologische, ethische und rechtswissenschaftliche Analysen (MuViT).\(^{264}\)

MOVIT deserves specific attention because it also considered ethical aspects and provided several guidelines. The country study of the United States will provide additional examples of project-based assessment methodologies for security solutions.

Examing in the results of security research projects appears to be an appropriate approach to enrich the work on advanced solutions for the European certification infrastructure in the security field. Therefore, this approach may also provide beneficial results in other security areas.

### 3.4.7. Summary and Conclusion

Germany is not only a key player in the European market for security PSS, but also a very diligent participant in European and international standardisation. It supports the priorities of a European Security Label, harmonisation of minimum requirements for the private operation of critical structures, certification of system integration and certification of security services, qualities that are considered a good practice. Germany has also an advanced security certification structure that is globally recognized and works to develop additional security-related documents at the national level in areas in which no European or international standards exist, effectively providing solutions to certification issues at the European level. For example, ARGE DIN 14675, which is currently an association of 10 accredited certification bodies and the owner of an accredited certification scheme working to connect stakeholders and produce updated and relevant security schemes in the field of ‘Fire Detection and Fire Alarm Systems’. This certification scheme, formed in response to a lack of an EU standard, is considered a good practice due to its collaborative nature.

Other good practices identified in Germany’s security-related infrastructure, which is comprised of both certified and non-certified CABs, include: ECB, which is based solely on European standards; Datenschutz certificate, that offers a variety of seals to address specific protection needs although building on national documents in most cases; and DAkkS that ensures the protection of highly sensitive and classified information by accrediting specific types of security schemes. Germany also continues to work to support the development of new security solutions and related evaluation approaches through publicly funded research.

Based on the highly advanced nature of security efforts in Germany, it is recommended that further efforts be made to analyse how CRISP can exploit the strengths of Germany’s security infrastructure in the development of the pan-European security scheme.

---

\(^{262}\) CamInSens, “Das Projekt CamInSens: Home”, no date. http://www.caminsens.org/index.html

\(^{263}\) More information is available at: Bundesministerium für Bildung und Forschung, ASEV, no date. http://www.bmbf.de/pubRD/Projektumriss_ASEV.pdf

\(^{264}\) More information is available at: Bundesministerium für Bildung und Forschung, ASEV, no date. http://www.bmbf.de/pubRD/Projektumriss_ASEV.pdf
3.4.8. REFERENCES


Bundesamt für Sicherheit in der Informationstechnik, Publikationen: Technische Richtlinien, no date. https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technische_richtlinien_node.html


DNVGL, “International Ship and Port Facility Security (ISPS) services”, no date.


VDE, “The mandate of the DKE”, no date.  
http://www.vde.com/en/dke/Aboutourselves/Pages/The%20Mandate%20of%20the%20DKE.aspx


3.4.9. ANNEX

Selected Security Technologies Associations and Networks:

- BHE – National Association of Manufacturers and Installers of Security Systems,
- BITKOM – Federal Association for Information Technology, Telecommunications and New Media,
- Future Urban Security,
- GESA – German European Security Association,
- SeSamBB – Security and Safety made in Berlin-Brandenburg,
- Secure Identity Berlin-Brandenburg,
- TeleTrusT – IT Security Association,
- VDE – Association for Electrical, Electronic & Information Technologies,
- ZVEI – Central Association for Electrical and Electronic Industry.

List of certification bodies accredited by DAKKS based on the search word security

Beschussamt Ulm Staatliche Prüf- und Zertifizierungsstelle für Waffen- und Sicherheitstechnik Prüflabor für Waffen- und Sicherheitstechnik, Albreße 74, 89081 Ulm
BAM Bundesanstalt für Materialforschung und -prüfung, BAM-Zertifizierungsstelle, Unter den Eichen 87, 12205 Berlin
Bundesamt für Sicherheit in der Informationstechnik; Fachbereich S2 - Zertifizierung und Standardisierung, Godesberger Allee 185-189; 53175 Bonn
CETECOM ICT Services GmbH, Untertürkheimer Straße 6-10; 66117 Saarbrücken
Comgroup GmbH, Drillberg 6, 97980 Bad Mergentheim
crashtest-service.com GmbH, Amelunxenstraße 30, 48167 Münster
datenschutz cert GmbH, Konsul-Smidt-Straße 88a, 28217 Bremen
DEKRA Certification GmbH, Handwerkstraße 15, 70565 Stuttgart
Deloitte Certification Services GmbH, Schwannstraße 6, 40476 Düsseldorf
DeuZert GmbH Deutsche Zertifizierung in Bildung und Wirtschaft, Freiheitstraße 124/126, 15745 Wildau
DIN CERTCO Gesellschaft für Konformitätsbewertung mbH, Alboinstraße 56, 12103 Berlin
DLG e. V. Testzentrum Technik & Betriebsmittel, Max-Eyth-Weg 1, 64823 Groß-Umstadt
DQS GmbH - Deutsche Gesellschaft zur Zertifizierung von Managementsystemen, August-Schanz-Straße 21, 60433 Frankfurt am Main
ECB European Certification Body GmbH, Lyoner Straße 18, 60528 Frankfurt am Main
EMCCons DR. RA?EK GmbH & Co. KG, Moggast, Boelwiese 8, 91320 Ebermannstadt
FGH GmbH, Hallenweg 40, 68219 Mannheim

---

265 GTAL, op cit., 2012, p. 3
Germanischer Lloyd SE Competence Centre Systems Certification, Brooktorkai 18, 20457 Hamburg
ift Rosenheim GmbH, Theodor-Gietl-Straße 7-9, 83026 Rosenheim
IndiKar Individual Karosseriebau GmbH Ballistik Prüflabor Indikar, Waldstraße 11, 08112 Wilkau-Haßlau
infaZ - Institut für Auditierung und Zertifizierung GmbH, Nixhütter Weg 85, 41468 Neuss
KPMG Cert GmbH Umweltgutachterorganisation, Barbarossaplatz 1a, 50674 Köln
m.dudde hochfrequenz-technik, Rottland 5a, 51429 Bergisch Gladbach
NavCert GmbH, Hermann-Blenk-Straße 22, 38108 Braunschweig
PERSICON Cert AG, Friedrichstraße 100, 10117 Berlin
Rheinmetall Waffe Munition GmbH Niederlassung Neuenburg "Prüflabor Chemie", Hans-Buck-Straße 1, 79395 Neuenburg
SGS Germany GmbH, Hofmannstraße 50, 81379 München
SGS-TÜV Saar GmbH Betriebsstätte München, Hofmannstraße 50, 81379 München
Siemens AG Test Center Erlangen/Karlsruhe Abteilung I IA CE SE R&D EMC, Günther-Scharowsky-Straße 21, 91058 Erlangen
T-Systems GEI GmbH Prüfstelle für IT-Sicherheit, Vorgebirgsstraße 49, 53119 Bonn
Technologiezentrum der Schüco International KG, Karolinenstraße 1-15, 33609 Bielefeld
TIC T-Systems Multimedia Solutions GmbH, Riesaer Straße 5, 01129 Dresden
TÜV AUSTRIA Deutschland GmbH, Pippinistr. 3, 82131 Gauting
TÜV Informationstechnik GmbH (TÜViT) Prüflabor für IT-Qualität, Langemarckstraße 20, 45141 Essen
TÜV Informationstechnik GmbH, Langemarckstraße 20; 45141 Essen
TÜV InterCert GmbH Group of TÜV Saarland, Am Bonner Bogen 2, 53227 Bonn
TÜV NORD CERT GmbH, Langemarckstraße 20, 45141 Essen
TÜV Rheinland Cert GmbH, Am Grauen Stein, 51105 Köln
TÜV Saarland e.V. TÜV SAAR CERT, Am TÜV 1, 66280 Sulzbach
TÜV SÜD Management Service GmbH, Ridlerstraße 65, 80339 München
TÜV SÜD Product Service GmbH, Sylvesterallee 2, 22525 Hamburg
TÜV SÜD Rail GmbH with offices in many cities, Barthstraße 16, 80339 München
TÜV Thüringen e. V. Zertifizierungsstelle für Systeme und Personal, Ernst-Ruska-Ring 6, 07745 Jena
TÜV-Zertifizierungsstelle der TÜV Technische Überwachung Hessen GmbH, Rüdesheimer Straße 119, 64285 Darmstadt
UIMCert GmbH, Moltkestraße 19, 42115 Wuppertal
VDE Prüf- und Zertifizierungsinstitut GmbH, Merianstraße 28, 63069 Offenbach
VdS Schadenverhütung GmbH, Amsterdamer Straße 174, 50735 Köln
(second entries of the same organisations deleted)
3.5. **POLAND**

3.5.1. **INTRODUCTION**

With 38.6 million inhabitants, Poland belongs to the group of the largest countries in Europe. Due to its geographic location, Poland’s security has specific relevance for Europe. This case study is mainly based on database research and web analyses. The database Perinorm was used to identify relevant national standards. In addition, the website of the Polskie Centrum Akredytacji [www.pca.gov.pl](http://www.pca.gov.pl) helped to identify significant certification organisations.

3.5.2. **SHORT DESCRIPTION OF POLAND’S SECURITY INDUSTRY**

The Polish security sector is relatively well developed, being quite strong in manufacturing mechanical security products. In addition, there are a few local companies producing sophisticated electronic equipment. There are also several companies with expertise in integrated systems, CCTV monitoring systems for cities and municipal transport, airport and railway security systems as well as intelligent building systems, access control biometric and chip technologies. Furthermore, 3,200 security service companies exist. Important segments of the market for security services include maritime security, Cash-In-Transit (CIT) as well as monitoring and remote surveillance. ECORYS works on new statistics of the European security industry in seven selected countries including Poland: UK, Italy, France, Spain, Poland, Estonia and Germany. The study will be published in summer 2015. Figure 35 provides preliminary data.

<table>
<thead>
<tr>
<th>Country</th>
<th>Turnover (billion €)</th>
<th>Employees (in 1,000)</th>
<th>Turnover/employee</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK</td>
<td>28.4</td>
<td>458</td>
<td>62</td>
</tr>
<tr>
<td>Italy</td>
<td>24.6</td>
<td>195</td>
<td>126</td>
</tr>
<tr>
<td>France</td>
<td>20.4</td>
<td>215</td>
<td>95</td>
</tr>
<tr>
<td>Spain</td>
<td>10.3</td>
<td>112</td>
<td>92</td>
</tr>
<tr>
<td>Poland</td>
<td>1.6</td>
<td>71</td>
<td>23</td>
</tr>
<tr>
<td>Estonia</td>
<td>1.3</td>
<td>26</td>
<td>50</td>
</tr>
<tr>
<td>Germany*</td>
<td>35.0</td>
<td>450</td>
<td>77</td>
</tr>
</tbody>
</table>

*source: German WISIND project

Source: Baker (2015), own notes based on the relevant presentation

Figure 35: Key figures of Poland’s security industry compared with other EU countries

The study shows the small size of the Polish security industry compared with other EU countries. The ECORYS report mentioned above will also provide Polish market data of specific

---

http://www.bpcc.org.pl/att/security.pdf,

267 UK Trade and Investment, op. cit., no date.

268 Confederation of European Security Services (CoESS), op. cit., 2011, data of 2011.

security products and services as well as information on the size of the companies. Compared with the other six countries in the ECORYS sample, the export orientation of the Polish security companies is relatively low. In contrast, the import of security products and solutions is of high importance.

According to the the CoESS facts and figures 2011, the annual turnover of private security service providers was € 1.5 bn in 2010. Although Baker’s (2015) estimated market volume of € 1.6 bn refers to the year 2015, this figure shows the importance of services in the security market. The annual turnover in this area builds on general guarding (excluding the segments listed hereafter): € 805.97 million, maritime security: € 4.50 million, Cash-In-Transit (CIT): € 454.77 million, monitoring and remote surveillance: € 198.12 million. The combined market share of the top three private security companies is 30%.

The research institute Frost & Sullivan has a specific focus on the demand side of the market, which surpasses the turnover of the domestic security companies due to imports. Regarding the future of Poland’s market for security solutions, this research institute formulated the optimistic prediction that the market is worth £ 2.5 bn (€ 3.4 bn) annually by 2015.

The Polish police, which is an important public player of the demand site for security solutions, is centralised. Its headquarters are in Warsaw and regional commands are located in all 16 provinces of Poland. The same centralised structure characterises border control, customs and fire services.

Public security and crime reduction are key governmental priorities and, although crime rates are decreasing, the public sector continues to be one of the largest buyers of security products. Poland has the EU’s longest external border. Strengthening public services responsible for border control has been one of the Polish government’s major objectives since 2008.

3.5.3. THE SECURITY STANDARDISATION FRAMEWORK

The key player in Poland’s standardisation system is the Polish Committee for Standardization (PKN). PKN is a State Organisational Unit financed by the State budget and recognised as a national standards body. It operates based on the Act on Standardisation of 12th September 2002, which specified basic goals, principles, organisation and financing of standards work and came into force on January 1st, 2003.

PKN approves national standard documents, which are adopted by consensus. It is publicly available and designed for voluntary, common and repeated use. In addition, it is marked - on an exclusive basis – with the acronym ’PN’. The following figure gives an overview of PKN’s TCs in the security field.

---

270 Baker, Paul, op. cit., 2015
274 Journal of Laws no. 169, item 1386
## Table of Security TCs

<table>
<thead>
<tr>
<th>TC</th>
<th>Polish name</th>
<th>English translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Osób Niepełnosprawnych</td>
<td>Disabled Persons</td>
</tr>
<tr>
<td>17</td>
<td>Pojazdów i Transportu Drogowego</td>
<td>Road Vehicles and Road Transport</td>
</tr>
<tr>
<td>18</td>
<td>Statków i Techniki Morskie</td>
<td>Ships and Marine Technology</td>
</tr>
<tr>
<td>19</td>
<td>Lotnictwa i Kosmonautyki</td>
<td>Aircraft and Space Vehicle Engineering</td>
</tr>
<tr>
<td>52</td>
<td>Systemów Alarmowych Włamania i Napadu</td>
<td>Alarm Systems</td>
</tr>
<tr>
<td>103</td>
<td>Urządzeń i Systemów Audio, Wideo i Podobnych</td>
<td>Audio, Video and Similar Systems and Equipment</td>
</tr>
<tr>
<td>105</td>
<td>Elektroakustyki oraz Rejestracji Dźwięku i Obrazu</td>
<td>Electroacoustics, Audio and Video Information Storage Systems</td>
</tr>
<tr>
<td>142</td>
<td>Geosyntetyków</td>
<td>Geosynthetics</td>
</tr>
<tr>
<td>172</td>
<td>Identyfikacji Osób, Podpisu Elektronicznego, Kart Elektronicznych oraz Powiązanych z nimi Systemów i Działań</td>
<td>Personal Identification, Electronic Signature and Cards and their Related Systems and Operations</td>
</tr>
<tr>
<td>173</td>
<td>Interfejsów i Budynkowych Systemów Elektronicznych</td>
<td>Interfaces and Building Electronic Systems</td>
</tr>
<tr>
<td>180</td>
<td>Bezpieczeństwa Pożarowego Obiektów</td>
<td>Fire Safety of Buildings</td>
</tr>
<tr>
<td>182</td>
<td>Ochrony Informacji w Systemach Teleinformacyjnych</td>
<td>Information Technology - Security Techniques</td>
</tr>
<tr>
<td>183</td>
<td>Bezpieczeństwa Urządzeń Informacyjnych, Telekomunikacyjnych i Biurowych</td>
<td>Safety of Information and Communication Technology and Business Equipment</td>
</tr>
<tr>
<td>244</td>
<td>Sprzętu, środków i Urządzeń Ratowniczo - Gaśniczych</td>
<td>Equipment for Fire Protection, Rescue and Fire Fighting</td>
</tr>
<tr>
<td>266</td>
<td>Aparatury Jądrowej</td>
<td>Nuclear Instrumentation</td>
</tr>
<tr>
<td>278</td>
<td>Wodociągów i Kanalizacji</td>
<td>Water Supply and Waste Water Engineering</td>
</tr>
<tr>
<td>280</td>
<td>Jakości Powietrza</td>
<td>Air Quality</td>
</tr>
<tr>
<td>297</td>
<td>Informacji Geograficznej</td>
<td>Geographic Information</td>
</tr>
<tr>
<td>302</td>
<td>Zastosowania Informatyki w Ochronie Zdrowia</td>
<td>Using of Informatics in the Health Protection</td>
</tr>
<tr>
<td>306</td>
<td>Bezpieczeństwa Powszechnego i Ochrony Ludności</td>
<td>Societal and Citizen Security</td>
</tr>
<tr>
<td>307</td>
<td>Zrównoważonego Budownictwa</td>
<td>Sustainability in Building Construction</td>
</tr>
<tr>
<td>308</td>
<td>Oceny Uwalniania Substancji Niebezpiecznych z Wyrobów Budowlanych</td>
<td>Assessment of Release of Dangerous Substances-Construction Products</td>
</tr>
<tr>
<td>309</td>
<td>Biometrii</td>
<td>Biometrics</td>
</tr>
<tr>
<td>311</td>
<td>Konserwacji Dób Kultury</td>
<td>Conservation of Cultural Property</td>
</tr>
<tr>
<td>314</td>
<td>Nanotechnologii</td>
<td>Nanotechnologies</td>
</tr>
<tr>
<td>501</td>
<td>Usług w Zakresie Systemów Bezpieczeństwa Pożarowego i Alarmowych Systemów Zabezpieczeń</td>
<td>Services for Fire Safety and Security Systems</td>
</tr>
<tr>
<td>505</td>
<td>Procesów Kryminalistycznych</td>
<td>Forensic science processes</td>
</tr>
</tbody>
</table>

Source: Own selection based on a figure from PKN
Figure 36: PKN’s TCs in the security field

The following figure shows Poland’s involvement in international security-related standardisation activities based on twelve examples.
Table 3:

<table>
<thead>
<tr>
<th>ISO TC</th>
<th>Topic</th>
<th>Participation (P/-O-Member)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC/JTC</td>
<td>Cards and personal identification</td>
<td>P</td>
</tr>
<tr>
<td>1/SC 17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO/IEC/JTC</td>
<td>IT Security techniques</td>
<td>P</td>
</tr>
<tr>
<td>1/SC 27</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO/IEC/JTC</td>
<td>Automatic identification and data capture techniques</td>
<td>-</td>
</tr>
<tr>
<td>1/SC 31</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO/IEC/JTC</td>
<td>Biometrics</td>
<td>P</td>
</tr>
<tr>
<td>1/SC 37</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO/TC 68</td>
<td>Financial services</td>
<td>O</td>
</tr>
<tr>
<td>ISO/TC 85</td>
<td>Nuclear energy, nuclear technologies, and radiological protection</td>
<td>O</td>
</tr>
<tr>
<td>ISO/TC 92</td>
<td>Fire safety</td>
<td>O</td>
</tr>
<tr>
<td>ISO/TC 223</td>
<td>Societal security</td>
<td>O</td>
</tr>
<tr>
<td>ISO/TC 224</td>
<td>Service activities relating to drinking water supply systems and</td>
<td>O</td>
</tr>
<tr>
<td></td>
<td>wastewater systems - Quality criteria of the service and performance indicators</td>
<td></td>
</tr>
<tr>
<td>ISO/TC 247</td>
<td>Fraud countermeasures and controls</td>
<td>O</td>
</tr>
<tr>
<td>ISO/PC 284</td>
<td>Management system for quality of private security company (PSC)</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>operations - Requirements with guidance</td>
<td></td>
</tr>
<tr>
<td>ISO/TC 292</td>
<td>Security</td>
<td>O</td>
</tr>
<tr>
<td>Total P+O</td>
<td></td>
<td>4+7</td>
</tr>
</tbody>
</table>

Source: Own analysis
Figure 37: Poland’s involvement in selected ISO/IEC TCs

According to Figure 37, Poland is more often operating as observer in international security standardisation at ISO than being an active contributor. This situation may be caused by the fact that Poland’s security industry is relatively small.

3.5.4. THE SECURITY CONFORMITY ASSESSMENT FRAMEWORK

Poland’s market for security certification reflects the small size of the domestic security industry. Regarding the private section of the Polish conformity assessment system, in particular two providers of security-related assessment services are important:275 CNBOP Centrum Naukowo – Badawcze Ochrony PrzeciwpoŜarowej (Scientific and Research Centre for Fire Protection) and TÜV SÜD Polska Sp. z o.o. Figure 38 shows that CIS offers additional services via its Czech office.

---

275 Based on a request, the national accreditation body PCA (Polish Centre for Accreditation) confirmed this statement.
### Certification of:

<table>
<thead>
<tr>
<th>Certification Body</th>
<th>Security products</th>
<th>Security systems</th>
<th>Security services</th>
<th>Others</th>
<th>Basis of the testing and certification processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNBOP</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>See a)</td>
</tr>
<tr>
<td>TÜV Süd</td>
<td>No answer</td>
<td>x</td>
<td>No answer</td>
<td>x (IT security)</td>
<td>See b)</td>
</tr>
<tr>
<td>CIS</td>
<td></td>
<td>x (IT security)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 38: Overview of security certification services in Poland

According to Lewis (2014),


It also provides “certification of quality systems for conformity with ISO 3834-2, -3, -4 (Quality requirements for fusion welding of metallic materials) and certification of Factory Production Control for conformity with the Construction Products Regulation (EU 305/2011), in the scope of steel and aluminium constructions”.

The Polish fire protection market is characterised by specific framework conditions. It is regulated by law, which relate mainly to products for the protection of life, property and the environment. The market for services in the area of fire protection is not regulated or controlled in a legal manner. Already undertaken initiatives of certifying service providers in the field of fire protection are voluntary.

Yet as a whole, while there are several standards for certification purposes for security (e.g IEC 62642, EN 50131, EN 50133, EN 50136, EN 50518 or the EN 54 series), none of the named have been used in the recent years.

#### 3.5.5. SELECTED SECURITY CERTIFICATION BODIES AND THEIR WORK

This chapter describes the activities of the CAB mentioned in the previous chapter in more detail.

---

276 Including IT security, risk management
277 Lewis, op. cit., 2014, p. 25
278 Lewis, op. cit., 2014, p. 25
279 Lewis, op. cit., 2014, p. 25
Centrum Naukowo - Badawcze Ochrony Przeciwpożarowej (CNBOP)

Accredited based on PN-EN 45011,281 CNBOP is one of the key providers of security-related certification services in Poland. The scope282 of its certification activities in the security field includes the areas of the ICS codes 13.220 (Protection against fire) and 13.340 (Protective equipment) and, with a broader focus, certification of construction products based on the EC decision 96/577/EC283 and Regulation 305/2011 (CPR).284 CNBOP frequently uses national standards for certification, e.g. in the field of ICS 13.220. The legal basis of the approval process includes in general:

- Conformity Assessment System Act of 30 August 2002 (JoL. No 166 item 1360 with amendments)
- Regulation of The Minister of Infrastructure of 8 November 2004 on Technical Approvals and organisational units authorized to deliver them (JoL. No. 249 item 2497 with amendments)

The relevant certification mark is shown below. CNBOP-PIB certification department carries out certification of admittance of products:

- used for ensuring public security or protecting health, life and property,
- introduced for the use in fire protection units and used by these units to alert in case of fire or other hazards, and to carry out rescue operations, as well as
- portable firefighting equipment.

Source: CNBOP
Figure 39: CNBOP’s certification mark

The department is accredited and notified for the certification of products on the basis of:

- EN 54-16 Voice alarm control and indicating equipment (VACIE)
- EN 54-24 Components of voice alarm systems – Loudspeakers and
- EN 54-4 Power supply equipment.

Additional certification services build, for example, on the standards285 PN-EN 54-2, -3, -5, -7, -10, -11, -12, -17, -18, -20, -21 and -23.

In addition, CNBOP-PIB offers voluntary certification of services, which provide protection against fire hazards.286 Voluntary certification is offered to service providers in the field of fire protection in compliance with the requirements of the European Association of Insurers

---

282 PCA, op. cit., no date.
285 PCA, op. cit., no date.
286 CNBOP, op. cit., no date.
D2.2: Consolidated report on security standards and certification

(Insurance Europe). 287 Insurance Europe unit chambers and insurance associations from 33 European countries including the Polish Chamber of Insurance (PIU). Its guidelines describe the process of services certification in the area of fixed firefighting systems in two documents:

- CEA 4046 *Base requirements for Installers of Fire Fighting Systems; September 2005*
- CEA 4047 *CEA Rules for the approval of Installers of Fire Fighting Systems in accordance with CEA 4046; September 2005*

CEA 4046 describes the basic requirements placed on firms to undertake activities related to the fixed fire-fighting systems while CEA 4047 includes guidelines for the certification body on how to carry out the process of certification of services.

CNBOP-PIB offers certification of services in the field of fixed firefighting systems including water (sprinkler, spray, mist), foam and gas.

Requirements in the relevant certification processes are mostly related to the formal and legal status of the service provider, organisational aspects, the existence of a certified quality management system according to ISO 9001, equipment, establishing and documenting carried out activities, qualifications of employed personnel, providing service / maintenance, insurance against civil liability in the field of carried out services, etc. But the most specific requirement is demonstrating practical fulfillment of some of the requirements in the specific area by impartial assessment. Figure 38 shows the main components of the relevant certification process.

![Figure 38: Elements of the relevant certification process](image)

Source: CNBOP

Figure 40: Elements of CNBOP’s certification of services

Information about mutual recognition agreements and international collaboration are not provided on CNBOP’s website. According to CRISP’s deliverable 2.1, there are many other

---

287 CNBOP, op. cit., no date.
European certification bodies, which offer services based on the EN 54 series. In this context, potential for further collaboration can be analysed.

TÜV SÜD Polska Sp. z o.o.

TÜV SÜD offers security system inspections. In addition, its auditing and system certification services in the security field include ISO 27001 - Information Security Management System as well as certificates for Risk Management and Safety Certificate Contractors (SCC).

CIS - Certification & Information Security Poland

CIS serves Poland via the office in Prague. As a recognised certification body, CIS - Certification & Information - Security GmbH is specialized in information security accreditation to ISO/IEC 27001 and IT service management accreditation to ISO/IEC 20000. The quality of CIS is awarded by BMWFJ (Federal Ministry for Economic Affairs, Family and Youth - AT).

According to standards.org, the international certification bodies Bureau Veritas Poland and Nippon Kaiji Kyokai (ClassNK) Poland also offer security certification services in Poland.

3.5.6. SUMMARY AND CONCLUSION

Poland’s security industry is relatively small in comparison to other Member States and no significant advanced certification approach was identified. Furthermore, only a limited number of certification bodies for the security field exist and the number of potential members of standardisation committees is limited - a fact reflected by the low level of standardisation activities on an international level.

CEA documents for security-related certification play an important role in Poland’s standards landscape. An appropriate co-existence of these documents with formal CEN/CENELEC standards in the European security certification landscape requires additional research.

3.5.7. REFERENCES


CNBOP, “Voluntary certification of services”, no date.

Journal of Laws no. 169, item 1386


PCA, “Details”, no date.  
https://www.pca.gov.pl/english/?page=karta_podmiotu_en&id=AC%20063

http://www.pkn.pl/en/standardization-system

TÜV SÜD, Auditing & System Certification, n.d.  

TÜV SÜD, Testing, Inspection and Certification Services, n.d.  

3.6. SLOVENIA

3.6.1. INTRODUCTION

Situated at a major transport crossroad and a member of the OECD since July 2010, Slovenia has an extremely high potential of economic development, which is however not yet fully exploited.

The key Slovene industries produce electrical equipment, electronics, trucks, chemicals, processed food, textiles, paper and paper products, and wood products. Ferrous metallurgy and rolling mill products, aluminium reduction and rolled products, and lead and zinc smelting are also developed. The economy is geared towards services, and Slovenia can boast top-class services in the field of information technology. It also has developed pharmaceutical and automobile manufacturing. Other major economic sectors include the food industry, electrical devices, metal processing, chemicals and tourism.

Slovenia’s trade is orientated towards other EU countries, mainly Germany, Austria, Italy, and France. The economy is highly dependent on foreign trade. This high level of openness makes it extremely sensitive to economic conditions in its main trading partners and changes in its international price competitiveness.

3.6.2. SLOVENIA’S SECURITY INDUSTRY

As it comes to large Slovenian companies in the security sector, there are two significant companies offering security services (Varnost Maribor and Sintal Concern). A third company, Iskra Sistemi, provides a wide range of security solutions, as well as products specialised for the energy sector and logistics.

Varnost Maribor d.d.290 with subsidiary companies in Croatia, Bosnia and Herzegovina, Serbia, Montenegro and Macedonia, employs over 2,000 people in Slovenia, has a € 28m sales turnover (in 2012) and controls more than 3,500 objects from its own control centre. They offer a complete range of services in the field of protection of persons, property, security engineering while also manufacturing upgrades for fire engines and vehicles intended for the transportation of valuables.291

Sintal Concern has almost 2,000 employees and an annual sales turnover of over 31m EUR (in 2012). Having a full national coverage and operating without any subcontractors of security services they offer integrated safety services for persons, premises and valuables.292

Iskra Sistemi d.d. is a global provider of industrial solutions and electrotechnical products. The company’s headquarters are in Slovenia, but they have markets all over the world and a subsidiary in India. Iskra Sistemi is the largest national company in the fields of process automation, communications and security systems for power distribution, transmission, networking, powerline communications, railway and road traffic and software solutions in the field of energy sector and logistics. They produce power capacitors, capacitors for use in elec-

290 “d.d.” refers to a public limited company
291 Varnost Maribor, O podjetju/About the company, no date. http://www.varnost.si/o_podjetju.
tronics, radio interference suppression components, switchgears, electrical measuring instruments, batteries, antennas, cores and potentiometers and offer services in the fields of galvanization, toolshop, electrical measuring laboratory and management and maintenance of buildings. They also offer consultancy, implementation and maintenance of technical security systems for private or business facilities and hold a license for designing security systems, a license for the implementation of technical security systems, a security clearance certificate of the Ministry of the Interior for the access to classified information of level INTERNAL, and a permission to carry out radiological activities.\footnote{Iskra sistemi, Podjetje/Company, no date. http://www.iskrasistemi.si/} 

The most notable SMEs in the security field can be divided between the following three groups:

- **Manufacturers:**
  - Spica International with its primary business area in access control,
  - Astel d.o.o.\footnote{"d. o. o." refers to the limited liability company} with its primary business area in CCTV,
  - Mars Commerce d.o.o. with its primary business area in communications;
- **Distributors:**
  - LOOP Maribor d.o.o. with its primary business area in CCTV,
  - Tenzor d.o.o. with its primary business area in CCTV;
- **Consultants:**
  - Palsit d.o.o. with its primary business area in information security management.

Spica International offers a wide choice of ID technologies, access control, and time and attendance systems. A network of Spica companies is one of the leading suppliers of data collection systems in South-East Europe with offices in five Adriatic countries.\footnote{Spica International, O nas/About us, no date. http://www.spica.si/o-nas/ekipa/vodstvo#} 

Astel d.o.o. is one of the leading manufacturers of video surveillance equipment. The company produces complete lines of matrix switchers, distribution amplifiers, twisted-pair systems, sequential switchers, keyboards and other CCTV electronics products.\footnote{Astel, About us/About us, no date. http://www.astel-cctv.com/about-us.html.} 

Mars Commerce d.o.o. operates in the field of automation and technical security facilities. Its business is the production, in particular of GSM products, representation of foreign companies selling equipment for automation and technical security equipment service and installation.\footnote{Mars Commerce, O podjetju/About the company, no date. http://www.mars-commerce.si/?str=o-podjetju.} 

Tenzor d.o.o. provides technical security services for retail shops, industry, telecommunication, banking, public administration as well as for private households. The company also performs security risk evaluations and consultancy.\footnote{Tenzor, Tenzor, no date. www.tenzor.si.} 

Palsit d.o.o. offers consulting and management in the field of information security.\footnote{Palsit, O nas/About us, no date. http://www.palsit.com/slo/podjetje.php.}
With the exception of Špica International, all the listed SMEs operate mostly only in Slovenia, which means that their international/European sales don’t play a significant role.

3.6.3. SECURITY STANDARDISATION FRAMEWORK

3.6.3.1. NATIONAL REGULATION ON STANDARDISATION

The legal bases for the establishment and performance of the independent national standards body and the performance of activities in the area of Slovenian national standardisation include:

- Standardisation Act (RS Official Gazette No. 59/1999),
- Decision on the establishment of the Slovenian Institute for Standardisation (SIST) (RS Official Gazette No. 70/2000 in 91/2002),
- Statutes of the Slovenian Institute for Standardisation and
- Decree on the notification procedures in the fields of standards, technical regulations and conformity assessment (RS Official Gazette No. 60/2000 and 35/2005).

3.6.3.2. NATIONAL STANDARDISATION BODY

Slovenia has one national standardisation body – the Slovenian Institute for Standardisation (SIST). SIST is a “sui generis” public institute founded by the Government of the Republic of Slovenia in August 2000 with the Decision on the establishment of SIST. The Standardisation Act of 1999 appointed SIST as a national standards body responsible for preparing and adopting voluntary standardisation documents, and representing the interests of Slovenia in the international and European standards organisations. SIST has to ensure equal involvement of all interested parties in standardisation activities thus enabling the co-development of European and international standardisation.

SIST is an active and full member of international (ISO and IEC) and European (CEN, CENELEC, ETSI) organisations for standardisation. According to Figure 41, SIST is a member of 3 security-related ISO TCs.

Activities of the SIST are performed pursuant to its annual work programme (which – among other – provides for the issuing of the Slovenian national standards included in the Programme of preparation of Slovenian national standards), adopted in agreement with the Government by the SIST Assembly, and the financial plan, approved in agreement with the Government by the SIST Council, in the public interest, with emphasis on professional independence. Both the annual work programs and the financial plans are published on its web page.

---

The Slovenian national standardisation system is directed and managed by the SIST Assembly consisting of the SIST members, who provide for the implementation of interests in the area of Slovenian national standardisation, and five representatives of the Government. The SIST President as a body represents SIST at the international and European levels, and chairs the Assembly and Council meetings. The Council as a management body has seven members, including two representatives of the SIST members, one representative of the employees, three representatives of the Government, and the SIST President. The SIST Director sees to the legality of SIST work and business operations and manages the SIST Secretariat, which is a technical/administrative service providing support to the SIST bodies and technical working bodies. The two Technical Boards – for the general field and for electrical technology, IT and telecommunications, respectively – are the bodies directing technical work in the field of national standardisation.

<table>
<thead>
<tr>
<th>ISO TC</th>
<th>Topic</th>
<th>Participation (P- / O- Member)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC/JTC 1/SC 17</td>
<td>Cards and personal identification</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 27</td>
<td>IT Security techniques</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 31</td>
<td>Automatic identification and data capture techniques</td>
<td>/</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 37</td>
<td>Biometrics</td>
<td>/</td>
</tr>
<tr>
<td>ISO/TC 68</td>
<td>Financial services</td>
<td>/</td>
</tr>
<tr>
<td>ISO/TC 85</td>
<td>Nuclear energy, nuclear technologies, and radiological protection</td>
<td>/</td>
</tr>
<tr>
<td>ISO/TC 92</td>
<td>Fire safety</td>
<td>O</td>
</tr>
<tr>
<td>ISO/TC 223</td>
<td>Societal security</td>
<td>/</td>
</tr>
<tr>
<td>ISO/TC 224</td>
<td>Service activities relating to drinking water supply systems and wastewater systems - Quality criteria of the service and performance indicators</td>
<td>/</td>
</tr>
<tr>
<td>ISO/TC 247</td>
<td>Fraud countermeasures and controls</td>
<td>/</td>
</tr>
<tr>
<td>ISO/PC 284</td>
<td>Management system for quality of private security company (PSC) operations - Requirements with guidance</td>
<td>/</td>
</tr>
<tr>
<td>ISO/TC 292</td>
<td>Security</td>
<td>/</td>
</tr>
<tr>
<td>Total P+O</td>
<td></td>
<td>3</td>
</tr>
</tbody>
</table>

Source: Own figure based on information provided on the ISO web page
Figure 41: SIST’s membership in security-related ISO TCs

The technical work is performed by 579 Slovenian experts, who as members of 77 SIST bodies set up for particular areas upon the initiative of interested parties preparing national standards and other documents (e.g. technical specifications, technical reports, and guides) and participate in the preparation of international and European standards as members of technical working bodies of the international and European organisations for standardisation.

Based on the SIST internal regulations related to the preparation, adoption and development of Slovenian standards, SIST publishes all draft national standards in public inquiries. After the conclusion of a public inquiry, all comments are collected and submitted to the corresponding SIST TC for further discussion. The period of public inquiry on draft national
standards lasts at least 30 days following the date of publication. In exceptional cases, the relevant TC may define a shorter period.\textsuperscript{304}

3.6.3.3. STANDARDS

In addition to European CEN/CENELEC/ETSI standards and international ISO/IEC/ITU standards, Slovenia has not set any national standards in the field of security. Furthermore, no national standards in the field of security were set substitutional to European CEN/CENELEC/ETSI standards and international ISO/IEC/ITU standards. Besides, no national standardisation projects in the field of security are currently on the way.

National regulation is however important for security standardisation activities in the following fields: private security service (based on Order of determining standards, obligatory in private security service\textsuperscript{305}), safety standards for court operations (based on rules of safety standards for court operations), requirements for safeguarding arms depots (based on rules of technical requirements for safeguarding arms depots, on rules pertaining to shooting ranges and on conditions for shooting) etc. All certification is based on existing European and international standards in this area.

SIST does not dispose of the information on specific security standards used for certification in Slovenia.

As provided by the Public Procurement Act,\textsuperscript{306} whenever possible, technical specifications listed in the public procurement tenders should be formulated referencing in order of preference to Slovenian standards transposing European standards, European technical approvals, common technical specifications, international standards, other technical reference systems established by the European standardisation bodies or, if those do not exist, to Slovenian standards, Slovenian technical approvals or Slovenian technical specifications relating to the design, calculation and execution of the works and use of the products.

Many EN standards are mandatory for private companies to be compliant with. Some examples are provided in Figure 42:


\textsuperscript{305} Ministry of the Interior, Order of determining standards, obligatory in private security service, Official Gazete of the RS, no. 24/12, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ODRE2132

\textsuperscript{306} In English available at www.dkom.si/mma/-/2007100210195957/.
<table>
<thead>
<tr>
<th>Standard</th>
<th>Regulation</th>
<th>Official Gazette No.</th>
<th>Competent authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIST EN 50131 - Intruder Alarm Systems</td>
<td>Order determining standards, obligatory in private security service</td>
<td>24/2012</td>
<td>Ministry of the Interior</td>
</tr>
<tr>
<td>SIST BS 5979:2005 - Remote centres receiving signals from security systems (incorporating Corrigendum No. 1)</td>
<td>Rules on safety standards for court operations</td>
<td>41/2007</td>
<td>Ministry of Justice</td>
</tr>
<tr>
<td>SIST EN 13631-7:2004 - Explosives for civil uses - High explosives - Part 7: Determination of safety and reliability at extreme temperatures</td>
<td>Rules on technical and safety requirements, forms and records concerning explosives and pyrotechnic products</td>
<td>105/2008</td>
<td>Ministry of the Interior</td>
</tr>
<tr>
<td>SIST EN 1143-1 - Secure storage units - Requirements, classification and methods of test for resistance to burglary - Part 1: Safes, ATM safes, strongroom doors and strongrooms</td>
<td>Rules on technical requirements for safeguarding arms depots, on rules pertaining to shooting ranges and on conditions for shooting</td>
<td>66/2001</td>
<td>Ministry of the Interior</td>
</tr>
<tr>
<td>SIST EN 1143 - Secure storage units - Requirements, classification and methods of test for resistance to burglary</td>
<td>Decision on the conditions for security equipment that may be installed in security areas</td>
<td>94/2006</td>
<td>Government Office for the Protection of Classified Information</td>
</tr>
<tr>
<td>SIST EN 356 - Glass in buildings - Security glazing - Testing and classification of resistance against manual attack</td>
<td>Decision on the conditions for security equipment that may be installed in security areas</td>
<td>94/2006</td>
<td>Government Office for the Protection of Classified Information</td>
</tr>
<tr>
<td>SIST EN 1300 - Secure storage units - Classification for high security locks according to their resistance to unauthorized opening</td>
<td>Decision on the conditions for security equipment that may be installed in security areas</td>
<td>94/2006</td>
<td>Government Office for the Protection of Classified Information</td>
</tr>
</tbody>
</table>

Source: SIST

Figure 42: List of some exemplary EN standards that are mandatory for private Slovenian companies to be compliant with

The use of mandatory standards is provided by the relevant law and is enforced by the competent inspection authority, which is also provided by (usually the same) law. Compliance with standards is demonstrated by test reports issued by the designated testing bodies, which are also tested by inspection authorities.  

---

307 Interview with SIST, 14 October 2014.
3.6.4. SECURITY CONFORMITY ASSESSMENT FRAMEWORK

There are three kinds of certification bodies responsible for conformity assessment in the security field:

- Certification bodies accredited by the national accreditation body - Slovenska akreditacija:
  - Slovenian Institute of Quality and Metrology (SIQ)
  - Slovenian national Building and Civil Engineering Institute (ZAG)
- Private certification bodies accredited by foreign accreditation bodies:
  - Bureau Veritas d.o.o. (accredited by COFRAC)
  - TÜV SÜD Sava d.o.o. (accredited by DAkkS)
- Governmental agencies:
  - Slovenian Roads Agency (body affiliated to the Ministry of Infrastructure and Spatial Planning)
  - Slovenian Traffic Safety Agency (public agency)
  - Public Agency of the Republic of Slovenia for Railway Transport (public agency)
  - Civil Aviation Agency of the Republic of Slovenia (public agency)
  - Energy Agency (public agency)
  - Slovenian Environment Agency (body affiliated to the Ministry of Agriculture and the Environment)
  - Slovenian Nuclear Safety Administration (body affiliated to the Ministry of Agriculture and the Environment)
  - Metrology Institute of the Republic of Slovenia (body affiliated to the Ministry of Economic Development and Technology)
  - Administration of the Republic of Slovenia for Civil Protection and Disaster Relief (body affiliated to the Ministry of Defense)

The national accreditation body responsible for the establishment, development and maintenance of a professional, independent and impartial accreditation system in Slovenia, and for the implementation of the related assignments, is Slovenska akreditacija (SA). SA was established by the Decision on the Establishment of Public Institute Slovenian Accreditation of the Government of the Republic of Slovenia.\(^{308}\) As a public institute with the state’s authorisation, it performs as the only independent and non-profit institution the assignments of a public service in the regulated and non-regulated sectors, and represents the interests of the Republic of Slovenia in the international accreditation organisations.

SA’s basic activity is accreditation of conformity assessment bodies. The Slovenian accreditation system complies with the requirements of the Regulation 765/2008 on accreditation and market surveillance. SA is organised and operates in compliance with the standard SIST EN ISO/IEC 17011:2004, and it complies with the rules of the international accreditation organisations. SA is a full member of EA and a member of ILAC and IAF.\(^{309}\)

\(^{308}\) Government of RS, Decision on the Establishment of Public Institute Slovenian Accreditation, Official Gazette, No. 36/00, 23/01, 121/04, 22/08, available at http://www.pisrs.si/Pis.web/pregledPredpisa?id=SKLE997

3.6.5. **SELECTED SECURITY CERTIFICATION BODIES AND THEIR WORK**

There are four relevant security certification bodies in Slovenia:

- Slovenian Institute of Quality and Metrology (SIQ),
- Slovenian national Building and Civil Engineering Institute (ZAG),
- Bureau Veritas d.o.o.,
- TÜV SÜD Sava d.o.o.

**SIQ**

SIQ is the main Slovenian security certification body accredited by the national accreditation body offering solutions in the fields of product testing and certification, management systems assessment, metrology, and training.  

### Kinds of PSS which are tested and certified in the security field

| ISO/IEC 27001 conformity (information security management) |

### Certification process(es) in the security area

Any organisation that has established a management system in line with the requirements of at least one management system standard can apply for certification. SIQ conducts audits and grants accredited certificates according to the requirements of the ISO/IEC 27001 standard in cooperation with Certification & Information Security from Vienna, Austria. The procedure consists of a documentation audit and a certification audit, conducted in two parts. The first part of a certification audit, focusing on the establishment and documentation of the information security management system which is usually not conducted on-site, encompasses:

- A review of the security policy and objectives;
- A review of the certification scope, supporting procedures and controls;
- A risk assessment report, implemented programmes and actions to reduce risks;
- A statement of applicability

The second part is carried out on-site and focuses on implementation of the system and its effectiveness, meeting the ISO/IEC 27001 standard requirements as well as legal and customer requirements. After awarding ISO/IEC 27001 certificate, the certification body annually conducts a surveillance audit of individual parts of the system to test whether the organisation still meets the requirements of the standard. A re-assessment of the entire system and its effectiveness is conducted once every three years. The certificate is valid for three years.

The certification and certificate maintenance procedure, as well as the activities of the parties involved in the procedure, are shown in the figure below.

---

Documents which form the basis of the testing and certification process(es)

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards</td>
<td>ISO/IEC 27001</td>
</tr>
<tr>
<td>Laws/regulations</td>
<td>Personal Data Protection Act</td>
</tr>
<tr>
<td>Internal guidelines/documents</td>
<td>/</td>
</tr>
<tr>
<td>Other documents</td>
<td>/</td>
</tr>
</tbody>
</table>

Security PSS which are certified based on the aforementioned standards

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product/technology/system/service</td>
<td>Information security management system</td>
</tr>
<tr>
<td>Standard(s) used in the certification process</td>
<td>ISO/IEC 27001</td>
</tr>
</tbody>
</table>
Security PSS which are certified based on any other aforementioned documents (laws/regulation, internal guidelines/documents etc.)

<table>
<thead>
<tr>
<th>Product/technology/system/service</th>
<th>Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data privacy</td>
<td>Personal Data Protection Act (just conformity not certification)</td>
</tr>
</tbody>
</table>

Quality seal

Key evaluation criteria in the security field and requirements for obtaining a certificate

<table>
<thead>
<tr>
<th>Product/technology/system/service: Information security management system</th>
<th>Evaluation criterion</th>
<th>Minimum requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC 27006</td>
<td>ISO/IEC 27001</td>
<td></td>
</tr>
</tbody>
</table>

Cooperation with external test laboratories in the security field

Involvement of the organisation in security standardisation

Yes.

Number of certificates issued in the security field annually

5-10

(Mutual recognition) agreements with other European countries/certification bodies in the security field

SIQ is a member of the IQNet and has an agreement with Certification & Information Security GmbH from Vienna.

Solutions for suppliers of certified security solutions from other European countries that wish to receive a certificate that is valid in the country

All certification companies under the IQNet mark can issue a valid certificate.

Summary

In the field of security certification (also in other fields not covered by this research) SIQ is the most relevant Slovenian certification body, having also its own quality seal which is very well-recognised and trusted. SIQ has affiliates in Croatia, Serbia, Italy and Germany. SIQ also issues internationally recognised IECEE/CB test reports and certificates and internationally recognised EMC reports that enable global market acceptance of products.
ZAG

ZAG is an independent, impartial and non-profit organisation, which fulfills all the requirements of the Directive No. 89/106 regarding approval bodies, which carry out the testing and attestation of conformity of construction products.\footnote{ZAG, About us, no date. http://old.zag.si/en/index.php?nav0=onas.} \footnote{The expression technical approval bodies is used by the Directive 89/106 on the approximation of laws, regulations and administrative provisions of the Member States relating to construction products Article 10 1. Each Member State shall notify the other Member States and the Commission of the names and addresses of the bodies which it has authorized to issue European technical approvals. 2. The approval bodies must satisfy the requirements of this Directive and in particular must be able: - to assess the fitness for use of new products on the basis of scientific and practical knowledge, - to take impartial decisions in relation to the interests of the manufacturers concerned or their agents, and - to collate the contributions of all the interested parties in a balanced assessment. 3. The list of approval bodies which are competent to issue European technical approvals, as well as any amendments to that list, shall be published in the‘G’ series of the Official Official Journal of the European Countries.}

<table>
<thead>
<tr>
<th>Kinds of PSS which are tested and certified in the security field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hydrants according to EN 14339 (underground fire hydrants) and EN 14384 (pillar fire hydrants).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Documents which form the basis of the testing and certification process(es)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standards</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Laws/regulations</strong></td>
</tr>
<tr>
<td><strong>Internal guidelines/documents</strong></td>
</tr>
<tr>
<td><strong>Other documents</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security PSS which are certified based on the aforementioned standards</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product/technology/system/service</strong></td>
</tr>
<tr>
<td>Underground fire hydrants</td>
</tr>
<tr>
<td>Pillar fire hydrants</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Quality seal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not for hydrants.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key evaluation criteria in the security field and requirements for obtaining a certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product/technology/system/service: Hydrants</strong></td>
</tr>
<tr>
<td><strong>Evaluation criterion</strong></td>
</tr>
<tr>
<td>In general</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cooperation with external test laboratories in the security field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at the moment (AVCP system 1).</td>
</tr>
</tbody>
</table>
Certification process(es) in the security area

(Mutual recognition) agreements with other European countries/certification bodies in the security field
No.

Summary
As an independent institute carrying out testing and attestation of conformity of construction products, ZAG performs only two security related certifications - based on standards EN 14339 and EN 14384.

Bureau Veritas d.o.o.

The company opened its affiliate in Slovenia in 1993 and operates today at three different locations: in Ljubljana, Maribor and in Koper.\(^{313}\)

Kinds of PSS which are tested and certified in the security field

- Financial services (Banks, Assurance, ...)
- Production services (Identity documents, Equipment production, ...)
- Service providers (Call centers; Integrators, Infrastructure providers; Hosting; Public, Private Mixed Cloud providers; Long and short term document storage; Software development in various sectors (Banks, Health; Certificate Agencies, ...)
- Public sector
- Educational sector

Certification process(es) in the security area
### Documents which form the basis of the testing and certification process(es)

| Standards | ISO/IEC 27001:2005  
| ISO/IEC 27001:2013 |
| Laws/regulations | All National (Slovene) and EU legislation and customer specific requirements. |
| Internal guidelines/documents | Documents related to the ISMS systems (e.g. Security policy; Risk assessment methodology; Risk assessment reports; Risk treatment plans, Statement of applicability, Information security policies; Work instructions, Software solutions and user guides and help, Internal rules against the Protection of Documents and Archives and Archival Institutions Act; Internal rules against the Personal Data Protection Act and other laws requirements (video control, data retention, ...)) |
| Other documents | Customer specific requirements and/or other country legislation depend on services that are provided by an organisation. |

### Security PSS which are certified based on the aforementioned standards

| Product/technology/system/service | Standard(s) used for certification |
| Banks | ISO/IEC 27001:2005  
ISO/IEC 27001:2013 |
| Software development | |
| Payment and settle systems | |
| Identity documents production | |
| Document management and retention services | |
| Hosting providers | |
| Cloud providers | |
| Call centre providers | |
| Goods production | |
| Access control and HRM solutions | |

### Security products/technologies/systems/services which are certified based on any other aforementioned documents (laws/regulation, internal guidelines/documents etc.)

| Product/technology/system/service | Documents |
| Banks | ISO/IEC 27001:2005  
ISO/IEC 27001:2013  
and related internal documents - criteria |
| Software development | |
| Payment and settle systems | |
| Identity documents production | |
| Document management and retention services | |
| Hosting providers | |
| Cloud providers | |
| Call centre providers | |
| Goods production | |
| Access control and HRM solutions | |
Quality seal

ISO 27001
BUREAU VERITAS
Certification

<table>
<thead>
<tr>
<th>Key evaluation criteria in the security field and requirements for obtaining a certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product/technology/system/service:</strong> Software development, hosting providers, banks</td>
</tr>
<tr>
<td><strong>Evaluation criterion</strong></td>
</tr>
<tr>
<td>Initial Audit and Certification Audit realised with IRCA trained Lead Auditor(s) under UKAS accredited schema</td>
</tr>
</tbody>
</table>

Cooperation with external test laboratories in the security field

None for the ISMS.

Involvement of the organisation in security standardisation

Yes, as an interested party during ISO standard preparing processes.

Number of certificates issued in the security field annually

Up to 5.

(Mutual recognition) agreements with other European countries/certification bodies in the security field

Global operation within Bureau Veritas company.

Solutions for suppliers of certified security solutions from other European countries that wish to receive a certificate that is valid in the country

If requested specific accreditation for specific country.

Summary

Bureau Veritas d.o.o. as a Slovenian affiliate of a large French group does only one security related certification – based on the ISO/IEC 27001 standard. Certifications of other security PSS are performed by its mother company.

Bureau Veritas d.o.o. reported a slight increase in the number of certifications of security solutions and highlighted the real need for security certification in the banking sector, public sector, telecom providers and especially in the health sector. As it comes to suggestions regarding the future of testing and certifying security solutions in Europe they highlighted the use of accredited, third party certification as completely independent fact and prove that certified organisation run operation on trusted level with guarantee for continuous improvement.
TÜV SÜD Sava d.o.o.

As a daughter company of the German Business Group TÜV SÜD AG, TÜV SÜD Sava provides its services in Slovenia, Croatia (subsidiary) and in Bosnia and Herzegovina (representing office). \(^{314}\)

### Kinds of PSS which are tested and certified in the security field

| ISO/IEC 27001 conformity (information security management) |

### Certification process(es) in the security area

<table>
<thead>
<tr>
<th>1. year</th>
<th>2. year</th>
<th>3. year</th>
<th>4. year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-Audit (optional)</td>
<td>Certification audit: in two stages</td>
<td>Surveillance audit</td>
<td>Surveillance audit</td>
</tr>
</tbody>
</table>

The first certification cycle consists of the certification audit and two surveillance audits. The second certification cycle (and all upcoming cycles) consists of a repeat audit and two surveillance audits.

- **Certification audit**
  - preparation, documentation review
  - audit stage 1
  - audit stage 2
  - preparation of the report and the preparation of necessary documentation
  - certificate

- **Surveillance audit**
  - preparation
  - audit
  - preparation of the report and the preparation of necessary documentation

- **Repeat audit**
  - preparation
  - audit
  - preparation of the report and verification of possible measures
  - certificate

### Audit:

#### Preparation:

The preparation includes the examination and the evaluation of the system documentation as well as the preparation and the reconciliation of the audit plan.

#### Audit:

Auditing by auditor (-s) in the organisation. Examination of practical use of the management system and verification of conformity with the audited standard and the performance assessment of the management system.

#### Documentation preparation:

Preparing the report and the verification of transferred corrective measures.

---

### Documents which form the basis of the testing and certification process(es)

<table>
<thead>
<tr>
<th>Standards</th>
<th>ISO/IEC 27001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laws/regulations</td>
<td>/</td>
</tr>
<tr>
<td>Internal guidelines/documents</td>
<td>/</td>
</tr>
<tr>
<td>Other documents</td>
<td>/</td>
</tr>
</tbody>
</table>

### Security PSS which are certified based on the aforementioned standards

<table>
<thead>
<tr>
<th>Product/technology/system/service</th>
<th>Standard(s) used in the certification process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information security management system</td>
<td>ISO/IEC 27001</td>
</tr>
</tbody>
</table>

### Quality seal

| / |

### Key evaluation criteria in the security field and requirements for obtaining a certificate

**Product/technology/system/service:** Information security management system

<table>
<thead>
<tr>
<th>Evaluation criterion</th>
<th>Minimum requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC 27006</td>
<td>ISO/IEC 27001</td>
</tr>
</tbody>
</table>

### Cooperation with external test laboratories in the security field

| / |

### Involvement of the organisation in security standardisation

Yes.

### Number of certificates issued in the security field annually

2

### (Mutual recognition) agreements with other European countries/certification bodies in the security field

| / |

### Solutions for suppliers of certified security solutions from other European countries that wish to receive a certificate that is valid in the country

| / |

### Summary

TÜV SÜD Sava d.o.o. as a Slovenian daughter company of a large German group does only one security related certification – based on the ISO/IEC 27001 standard. Certifications of other security PSS are performed by its mother company.
3.6.6. **SUMMARY AND CONCLUSION**

Slovenia, as one of the smallest EU Member States, does not have a strong and export oriented security industry. The only relevant companies, whose international and European sales play a significant role, are Iskra Sistemi and Spica International. The majority of relevant large companies in the sector focus on private security services. The biggest and most varied part of the security industry represents SMEs.

The national standardisation framework is built around the national standardisation body SIST. Slovenia has not set any national standards in the field of security, neither in addition nor substitutional of the existing European CEN/CENELEC/ETSI standards and international ISO/IEC/ITU standards. This is mostly a result of the small internal market and financial constraints of SIST. An interesting aspect is that foreign national standards can build the foundation for mandatory standards in Slovenia. SIST BS 5979:2005, shown in Figure 42 provides an example for that.

Based on legislation, technical specifications listed in the public procurement tenders should be, whenever possible, formulated by referencing to the existing standards. The legislation also provides for private companies to be compliant with some EN standards e.g. in the areas of private security services, safety standards for court operations, requirements for safeguarding arm depots, concerning explosive and pyrotechnic products and security equipment to be installed in security areas.

The security conformity assessment framework is built around two certification bodies – institutes accredited by the national accreditation body (SIQ and ZAG) and two private certification bodies accredited by foreign accreditation bodies (TÜV SÜD Sava d.o.o. and Bureau Veritas d.o.o.).

The majority of certifications in the security field are based on ISO/IEC 27001 standard (information security management). The certification processes of TÜV SÜD Sava d.o.o. and Bureau Veritas d.o.o. were shown in detail. Both concepts include surveillance audits, two and three years after the first certification took place, while an additional audit is necessary to start a new certification cycle in the fourth year.

3.6.7. **REFERENCES**


Government of RS, Decision on the Establishment of Public Institute Slovenian Accreditation, Official Gazette, No. 36/00, 23/01, 121/04, 22/08, available at http://www.pisrs.si/Pis.web/pregledPredpisa?id=SKLE997

Interview with Bureau Veritas d.o.o., 27 October 2014.

Interview with SIQ, 2 October 2014.

Interview with SIST, 14 October 2014.
Interview with TÜV SÜD Sava d.o.o., 27 October 2014.

Interview with ZAG, 23 October 2014.

Iskra sistemi, Podjetje/Company, no date.
http://www.iskrasistemi.si/.

Mars Commerce, O podjetju/About the company, no date.
http://www.mars-commerce.si/?str=o-podjetju.

Ministry of the Interior, Order of determining standards, obligatory in private security service, Official Gazete of the RS, no. 24/12,
http://www.pisrs.si/Pis.web/pregledPredpisa?id=ODRE2132

Palsit, O nas/About us, no date.

Sintal koncern, O nas/About us, no date.
http://www.sintal.si/o-nas/.


Slovenski inštitut za standardizacijo (SIST), O SIST/About SIST, no date.

Špica International, O nas/About us, no date.
http://www.spica.si/o-nas/ekipa/vodstvo#.

Tenzor, Tenzor, no date. www.tenzor.si.


Varnost Maribor, O podjetju/About the company, no date.
http://www.varnost.si/o_podjetju.

ZAG, About us, no date.
3.7. SPAIN

3.7.1. INTRODUCTION

This chapter presents the current state of standardisation and certification on security in Spain. The starting point is based on interviews with representatives of some of the most important certification companies in Spain. These companies belong to multinational firms but their contribution has been very important, as they have affected the characteristics of the Spanish market. Analysis of the Spanish security standardisation and certification system has not been carried out previously by Spanish researchers. Thus, the main resources, which this study draws on has been analysis of standards for the certification of security products, services or systems. In addition, the websites of the Spanish accreditation body ENAC and of the Spanish certification and standardisation body AENOR have been essential tools. The websites of companies that certify against some security standards have also been useful. Publications of government agencies - such as ministries and directorates also provided helpful sources of information.

3.7.2. SHORT DESCRIPTION OF THE SPANISH SECURITY INDUSTRY

From a report by the U.S. Department of Commerce (U.S. Commercial Service) the following information can be obtained: In general, the Spanish Safety and Security industry is highly competitive. Due to Spain being an open economy there are competitors from all over the world. At hand with the economic context of Spain, e.g. the end of the residential construction boom and austerity measures the industry was expected to decrease in 2013, above all affecting the safety equipment industry. Contrary to that, cyber security grows considerably and is getting a more central role. Other markets that are expected to remain important are explosives detection, equipment for scientific police and high-end surveillance systems and consumer-focused security solutions like IP video surveillance. Wildfire firefighting equipment and services are also in demand. Apart from that, a trend towards more integrated solutions can be observed.

Currently, no specific additional statistics of Spain’s security industry exist on a European level. One reason for this lack of data is that the security industry comprises many technical areas and related products and services, such as CCTV, alarm systems and aviation security services. Based on this diversity, the industry is not included in NACE and Prodcom. In addition, domestic market studies of the different Member States are often not comparable due to different national definitions of the market for security solutions. The European Commission is aware of the lack of additional data and entrusted ECORYS with a market study of key European countries which will also include Spain. The study will be completed in summer 2015. According to preliminary data, the turnover of Spain’s security industry is € 10.32 bn, which is accomplished with 112,000 employees (see country study ‘Poland’).

---

318 Eurostat statistics for Manufactured goods
3.7.3. **The Security Standardisation Framework**

### 3.7.3.1. Asociación Española de Normalización y Certificación (AENOR)

This section provides information on AENOR. It was founded in 1986, coinciding with Spain’s accession to the European Economic Community. AENOR is responsible for developing technical standards and certifying products, services and companies. As single existing agency in Spain processing “UNE standards”, AENOR has 200 technical standardisation committees. The Spanish technical standards catalogue includes more than 28,000 standards, more than 90,000 products feature the N Mark and more than 60,000 management system certificates have been issued. AENOR is also among the 10 most important certification organisations in the world. AENOR’s international activities in selected ISO committees are shown in the following figure.

<table>
<thead>
<tr>
<th>ISO TC</th>
<th>Topic</th>
<th>Participation (P-/O-Member)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC/JTC 1/SC 17</td>
<td>Cards and personal identification</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 27</td>
<td>IT Security techniques</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 31</td>
<td>Automatic identification and data capture techniques</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 37</td>
<td>Biometrics</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 68</td>
<td>Financial services</td>
<td>O</td>
</tr>
<tr>
<td>ISO/TC 85</td>
<td>Nuclear energy, nuclear technologies, and radiological protection</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 92</td>
<td>Fire security</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 223</td>
<td>Societal security</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 224</td>
<td>Service activities relating to drinking water supply systems and wastewater systems - Quality criteria of the service and performance indicators</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 247</td>
<td>Fraud countermeasures and controls</td>
<td>P</td>
</tr>
<tr>
<td>ISO/PC 284</td>
<td>Management system for quality of private security company (PSC) operations - Requirements with guidance</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 292</td>
<td>Security</td>
<td>-</td>
</tr>
</tbody>
</table>

Total P+O: 10+1

Source: ISO official website

Figure 43: Spain’s participation in selected ISO TCs

---

319 They are similar to EN or ISO standards but are created and approved by AENOR for the Spanish market. UNA stands for “Una Norma Española” as recognized by the First Additional Provision of Royal Decree 2200/1995.

320 This information is available on the following sources:


AENOR website: http://www.en.aenor.es/aenor/aenor/perfil/perfil.asp#.VR2ejpOsX8Q


http://www.iso.org/iso/about/iso_members/iso_member_participation_tc.htm?member_id=1717
The figure shows that AENOR is not only an active player on a national level but also in international security standardisation.

AENOR is responsible for creating new standards for the Spanish market or to transpose European standards into UNE and its subsequent dissemination, distribution, promotion and marketing. UNE standards are not binding but a law, a regulation or a royal decree may be created based on these standards. UNE standards are developed within a TC for Standardisation (CTN) based on the following phases:

- Assembly preparations.
- Development of the draft standard.
- The proposed standard is developed in consultation with experts and stakeholders.
- TC proceeds to study them and approves the proposed final standard for consideration and adoption by AENOR.
- Ultimately, it proceeds to the registration, publication and distribution of the UNE standard in the BOE.322

- The standards can be promoted and marketed by relevant organisations.

On the other hand, the Coordinating Council of Industrial Security completes the Spanish standardisation framework.323 This is an administrative body established under Article 18 of the Law of Industry, and under the Ministry of Industry, Trade and Tourism that promotes and coordinates the criteria and actions of public authorities in the field of industrial security. In addition, it encourages coordination of actions among the subjects of security and industrial quality.324

### 3.7.3.2. The Aviation Safety and Security Agency AESA and Accredited Organisations

AESA is the state body that ensures that civil aviation standards are observed in all aeronautical activity in Spain. It takes on responsibility for: aviation security, certification, maintenance, licenses, operations, aircraft registration records, aerial works, aviation security, interoperability, single European sky, etc. They work to ensure that aviation security and security and transport standards in Spain are observed, to promote the development, establishment and application of national and international laws on air security and passenger protection, to implement a safety and security culture and to protect the passenger rights agents and society.325

---

324 The distinction between security and industrial grade is the following: the first regulates the exercise of administrative activity of industrial control; the second, however, is no more than a legal recognition of private activities that are in the Industry Act.
http://www.seguridadaerea.gob.es/media/3999114/cuadriptico_aesa_ingles.pdf
Accredited bodies by AESA (June 2014)

- **AENA**[^326] is responsible for managing and controlling air traffic, aeronautical information and the communications, navigation and surveillance networks needed to ensure that airlines and their aircraft fly in a safe, smooth and orderly manner in and through Spanish airspace.

The publication of *Law 9/2010 of April 14th*[^327] establishes a new general activity framework for air navigation in Spain. It determines the obligation of the civil providers of such services and lays down certain working conditions for the civil air traffic controllers, AENA is the Spanish company designated by the State to supply air traffic services during the en route and approach phases.

Air traffic service at Spanish airports has been deregulated to allow the entry of other operators besides AENA.

- **INECO**[^328] (certification supplier for Air Traffic Service, hereinafter, ATS) has participated in the process of expansion and modernisation of the entire Spanish airports system. It optimises air transport to improve mobility and offers complete services to organisations from the consulting phase to the commissioning operation.

- **SAERCO**[^329] (certification supplier for ATS, communication, navigation and supervision) is a company formed by a group of professionals from the world of aviation and air navigation. Its main objective is to provide air navigation services that include air traffic control (ATC) in airfields, airports and control centres, as well as other associated air traffic services (ATS) such as flight information services and advisory service. All services comply with the European regulatory framework of Single European Sky, the Common Requirements for the Provision of Air Navigation Services (EU Regulation 1035/2011), the Spanish Air Transit Regulations (Royal Decree 57/2002), and other International Civil Aviation regulations concerning air navigation services.

- **FerroNATS Air Traffic Services**[^330] (certification supplier for ATS) is the joint venture between Ferrovial Servicios (Spanish company which operates within the industry of infrastructure management through its different divisions: airports, construction, toll roads and services) and NATS (the UK’s provider of air traffic services and solutions). It combines Ferrovial Servicios’ knowledge about airport management and the customer and the operational air traffic control management expertise of NATS.

These organisations provide, for example, certification for Airport and aviation security services based on UNE-EN 16082. The National Cryptologic Centre (CCN) Spain’s National Cryptologic Centre (CCN) is responsible for the security of information technologies and the protection of classified information. It certifies the security of information technology products or systems in accordance with a legal framework (Spanish[^331] and European[^332] legislation

[^326]: AENA’s official website is available at: http://www.aena.es/csee/Satellite/HomeAena

[^327]: Publication of the mentioned law is available on: http://noticias.juridicas.com/base_datos/Admin/l9-2010.html

[^328]: INECO’s official website is www.ineco.com/webineco/en/what-we-do/markets


related to the areas of personal data protection, consumer protection, electronic signature and information society) and documents that rule the internal operation of the Certification Body. But, in turn, one of CCN’s most remarkable duties is to develop and disseminate standards, instructions, guidelines and recommendations to ensure the security of the information and communications technology from the administration, embodied in the series of CCN-STIC documents.

One of the principles established by law 11/2007 of 22 June, on electronic access of citizens to services public in Article 42.2 of the National Insurance Scheme is to provide a framework to establish the necessary conditions of confidence in the use of electronic media is also Royal Decree 3/2010 of January 8th regulates the National Security Framework. It sets the basic principles and minimum requirements and protective measures to be implemented in systems administration, and promotes the development and dissemination of security guides in order to facilitate better compliance with these minimum requirements.

The rules of Cryptologic Certification are based on the CCN-STIC Guides. To obtain the certificate, the product must already have a Common Criteria certificate. The corresponding technical evaluation report is first delivered to the National Cryptologic Centre. Subsequently, the cryptology evaluation is carried out, during which the analysis of the encryption algorithms, security mechanisms and the proper functioning of the equipment is taken into account. The equipment is then assigned the maximum level of information classification for which it is authorized to handle.

Documents for functional certification (for products and systems)

The criteria and methodology for evaluation, in the current versions used by the Body of Certification are:

- ITSEC/ITSEM
  - ITSEC v1.2, June 1991
  - ITSEM v1.0, September 1993
Documents for cryptologic certification

The rules of Cryptologic Certification are based on the CCN-STIC Guides. The most important guides are:

- 000 Series: Policies
  - CCN-STIC-001 Security of ICT in Public Administration
  - CCN-STIC-002 Cryptologic Coordination in Public Administration
  - CCN-STIC-003 Use of Certified Ciphers
- 100 Series: Procedures. The CCN-STIC-100 Series provides a common framework for action in the accreditation process, TEMPEST\textsuperscript{335} certification, material management number and any other field under consideration.
  - CCN-STIC-101 National Accreditation Procedure
  - CCN-STIC-103 Catalog of Certified Products
  - CCN-STIC-150 Evaluation and Classification of Ciphers with Cryptologic Certification
  - CCN-STIC-151 TEMPEST Evaluation and Classification for Equipment
  - CCN-STIC-152 Local Zoning Evaluation and Classification
  - CCN-STIC-153 Evaluation and Classification of Shielded Cabinets
- 400 Series: General Guides. The CCN-STIC-400 Series includes recommendations for security officials on specific aspects of ICT security (perimeter security, wireless, mobile, security tools, etc.).

**Addendum: documents for TEMPEST certification in Spain**

As an example, this section provides information on Spain’s use of specific international ICT standards and the related certification scheme TEMPEST which is implemented in selected countries. Since the main focus of the CRISP project is not on TEMPEST-related ICT aspects, this report outlines the framework conditions of the TEMPEST certification in one Member State only without describing the TEMPEST framework in detail.

\textsuperscript{335} See next section
TEMPEST is a specific certification scheme for ICT security products from the U.S. American National Security Agency and the NATO. Many specifics of the TEMPEST standards are classified. In order to implement procedures that optimise the implementation costs connected with TEMPEST measures, NATO has developed several documents through the SECAN (Systems Security and Evaluation Agency). Such documents are the standard used for the equipment and systems evaluation in the laboratory, for the procedures linked to TEMPEST evaluation of platforms, for procedures aimed at ZONING evaluation and classification of installations and for guidelines on systems evaluation.

The EU Council has developed the corresponding regulations regarding the areas of its competence. Such documents were based on the example of the already existing NATO documents and they aim to harmonize both the needed measures and the procedures to carry them out. According to CCN, the documents that have been used to develop the national TEMPEST regulation are based on the following NATO and EU documents:

- SDIP-27/1 NATO TEMPEST Requirements (NC)
- SDIP-28/1 NATO ZONING Procedures (NR)
- SDIP-29/1 Facility Design Criteria and Installation of Equipment for the Processing of Classified Information) (NR)
- IASG-07 TEMPEST Basic Principles (R-UE)
- IASG-07-01 Selection and Installation of TEMPEST Equipment (R-UE)
- IASG-07-02 TEMPEST ZONING Procedures (R-UE)
- IASG-07-03 EU TEMPEST Requirements and Evaluation Procedures (C-UE)

The rules of TEMPEST Certification are based on the following CCN-STIC Guides:

- CCN-STIC-004 TEMPEST Policy (DL)
- CCN-STIC-150 TEMPEST Evaluation and Certification of encryptors with Cryptologic Certification
- CCN-STIC-151 TEMPEST Evaluation and Certification of de Equipment
- CCN-STIC-152 ZONING Evaluation and Classification of Rooms
- CCN-STIC-153 Evaluation and Certification of Shielded Cabinets
- CCN-STIC-154 TEMPEST Protection Measures of Installations

Additional information on EU TEMPEST certification is provided in chapter 3.7.5.

3.7.4. **THE SECURITY CONFORMITY ASSESSMENT FRAMEWORK**

This sub-chapter represents Spain’s accreditation body ENAC as well as important certification bodies.

**Spain’s accreditation body ENAC**

ENAC's mission is to build confidence in the market for customers, manufacturers, resellers and other stakeholders. This includes in particular contributing to the safety and welfare of the public. ZONING is an equipment classification based on OTAN equivalent requirements.

---

336 ZONING is an equipment classification based on OTAN equivalent requirements.

basados en los equivalentes de OTAN, si bien los equipos pueden ser clasificados como ZONA 1 a ZONA 3.

337 CCN, “Documents”, no date.

people, to the quality of products and services as well as to the protection of the environment. It also aims at increasing the competitiveness of Spanish products and services and lowering costs for the society. ENAC’s origin was the Spanish Network of Laboratories RELE, created in 1986. Since chapter 3.7.3.1 introduced AENOR, another important player in Spain’s quality infrastructure, the following figure differentiates between both organisations.

<table>
<thead>
<tr>
<th>Relevant institutions</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENAC</td>
<td>The National Accreditation is the body designated by Spain’s Administration to establish and maintain the nationwide accreditation system according to international standards based on EU policies and recommendations.</td>
</tr>
<tr>
<td>AENOR</td>
<td>AENOR is the Spanish standardisation body responsible for the development and dissemination of technical standards. It also takes the certification activity.</td>
</tr>
</tbody>
</table>

Figure 44: Key organisations in Spain’s security-related conformity assessment framework

ENAC’s performance is supervised by the Administration in addition to others international accreditation bodies that indirectly perform accreditation bodies in other countries. They are linked by mutual recognition agreements.\(^{338}\)

**Security standards used by accredited certification bodies in Spain**

This section provides an overview of the use of selected security standards by certification bodies in Spain.

---

\(^{338}\) Internationally, ENAC is a member of the organisations European Accreditation (EA) and International Accreditation Forum (IAF), organizations that have signed agreements on mutual recognition of accreditation issued by any of its members.
<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
<th>CABs which offer certification based on the standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN 54 - series</td>
<td>Fire detection</td>
<td>AENOR, Bureau Veritas Certiveria, LGAI Technological Center Alter Technology TÜV NORD, s.a.</td>
</tr>
<tr>
<td>EN 50131 (UNE-EN 51031)</td>
<td>Intrusion detection</td>
<td>Alter Technology TÜV NORD, s.a. LGAI Technological Center</td>
</tr>
<tr>
<td>(EN 16763)</td>
<td>Services for fire security (fire detection, voice alarm, intrude alarm, access control, smoke and heat exhaust, ventilation, CCTV systems, control equipment for escape)</td>
<td>Asistencia Técnica Industrial (une), Cualcontrol-ACIECA, Entidad Colaboradora de la Administración, Enmacosa, Eurocontrol (une), In- Berco Inspección y control, Ingeniería de Gestión Industrial (une), Ingeniería y Técnicas de Calidad, Marsan Ingenieros, s.l., Oca Inspección Control y Prevención (une) Simecal, Servicios de Control e Inspección, SGS (une), TÜV (une)339</td>
</tr>
<tr>
<td>EN 16747 ISO 20858:2007</td>
<td>Maritime and port security services</td>
<td>AENOR</td>
</tr>
<tr>
<td>EN 16352</td>
<td>Specifications for reporting crime incidents</td>
<td>Information not found</td>
</tr>
<tr>
<td>EN 14383</td>
<td>Crime prevention through building, facility and area design</td>
<td>Information not found</td>
</tr>
</tbody>
</table>

339 The above institutions do not certify that standard but the following rules: UNE 192005: Procedure for regulatory inspection. Fire security in industrial plants. RD N. 1942/1993 (BOE 14/12/1993) amending facilities approved fire protection Regulation.
### Standards with specific information from ENAC

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
<th>CABs which offer certification based on the standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 28000</td>
<td>Supply chain security</td>
<td>AENOR, TÜV Rheinland, DNV Business Assurance, Bureau Veritas España, OCACERT, SGS…</td>
</tr>
<tr>
<td>EN ISO 22301</td>
<td>Societal security. Business continuity management systems. Requirements</td>
<td>Ibermática, Bureau Veritas España, SGS</td>
</tr>
<tr>
<td>EN 13094&lt;sup&gt;(1)&lt;/sup&gt;</td>
<td>Tanks for the transport of dangerous goods</td>
<td>Applus norcontrol S. L. (unipersonal), Asistencia Técnica Industrial, Cualicontrol – ACI, ECA, Eurocontrol, Ingeniería de Gestión Industrial, Ingeniería y Técnicas de Calidad, Oca Inspección Control y Prevención, Simecal, Servicios de Control e Inspección, SGS, TÜV - They certify similar standards but EN 13094 has never been certified.</td>
</tr>
<tr>
<td>EN 14025&lt;sup&gt;(2)&lt;/sup&gt;</td>
<td>Tanks for the transport of dangerous goods. Metallic pressure tanks. Design and construction</td>
<td>Applus norcontrol S. L. (unipersonal), Asistencia Técnica Industrial, Cualicontrol – ACI, ECA, Eurocontrol, Ingeniería de Gestión Industrial, Ingeniería y Técnicas de Calidad, Oca Inspección Control y Prevención, Simecal, Servicios de Control e Inspección, SGS, TÜV</td>
</tr>
<tr>
<td>EN 12972&lt;sup&gt;(3)&lt;/sup&gt;</td>
<td>Tanks for transport of dangerous goods. Testing, inspection and marking of metallic tanks</td>
<td>Applus norcontrol S. L. (unipersonal), Asistencia Técnica Industrial, Cualicontrol – ACI, ECA, Eurocontrol, Ingeniería de Gestión Industrial, Ingeniería y Técnicas de Calidad, Oca Inspección Control y Prevención, Simecal, Servicios de Control e Inspección, SGS, TÜV - They certify similar standards but EN 12972 has never been certified.</td>
</tr>
<tr>
<td>EN 14339</td>
<td>Underground fire hydrants</td>
<td>AENOR, Bureau Veritas Certiveria, LGAI Technological Center</td>
</tr>
<tr>
<td>EN 14384</td>
<td>Underground fire hydrants</td>
<td>AENOR, Bureau Veritas Certiveria, LGAI Technological Center</td>
</tr>
</tbody>
</table>

<sup>(1)</sup> <sup>(2)</sup> <sup>(3)</sup> No certification bodies certify the above-mentioned standards. These standards are certified on the basis of European Agreement concerning the transport of dangerous goods by road (ADR), 09.30.1957 in Geneva (revised text) and Order (September 20, 1985, BOE 27/09/1985) on construction standards, type approval, testing and inspection of tanks for the carriage of dangerous goods, and subsequent amendments.

---

Figure 45: Accredited Spanish certification bodies for selected security standards
The figure shows AENOR’s importance not only in standardisation but also in the field of security certification. In addition, it unveils many areas in which AENOR is also the only provider of security certification in Spain.

Selected security certification bodies and their work

There are three types of certification bodies in Spain. Accredited private certification bodies are the most common but there are non-accredited private certification bodies and government agencies as well. Spanish certification bodies are organisations that assess conformance and certify compliance with a reference standard, either the product, service or management system of an organisation. They issue certificates and reports of conformity assessment. Certification bodies must be independent of the organisation they audit, and should not have done other work for it, such as advisory to implement the system they certify. The following figure provides an overview of private certification bodies in Spain.

<table>
<thead>
<tr>
<th>Certification of:</th>
<th>Security products</th>
<th>Security systems</th>
<th>Security services</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Body:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applus+ Spain</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BMC Certification Spain</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AENOR International Spain</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bureau Veritas Spain</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SGS Spain</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TUV Rheinland Spain</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Own figure
Figure 46: Overview of selected CABs in the security field in Spain

Addendum: Selected marks in the privacy field

In Spain, privacy seals and marks (known as distintivos públicos de confianza) are regulated by the 3rd Final Disposition of Royal Decree 231/2008 of 15 February. They are graphic mechanisms provided by a promoter that previously has certified compliance with a code of conduct default.

Confianza online

This seal is the most widely popular in Spain as it offers comprehensive protection in accordance with its Code of Ethics. In this way it provides a mechanism at the time of handling claims through two bodies:

- The Jurado de la Publicidad de AUTOCONTROL340, for all matters relating to commercial communication, privacy, data protection and child protection.

---

340 It is an independent body created to fulfill the principles of Community Recommendation 98/257/EC of 30 March 1998 on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes and the role of settling disputes at the request of the parties, or third parties on any issue regarding advertising.
The National Consumer Arbitration Board to contractual issues with consumers, after mediation attempt by the Spanish Association of Digital Economy (adigital).

It is not a requirement that companies or organisations that apply for a membership of *Confianza Online* sell a product or service in the market, but they have to express a commitment to comply with the Ethic Code.\(^\text{341}\)

**Trusted Shops**

Is Europe’s leading specialist in the certification of online shops. This company carries audits in accordance with more than 70 individual and depending on the results criteria, given the quality seal.\(^\text{342}\)

**AENOR mark for a Better Business Practices for Electronic Commerce**

This is the first precedent of distinctive public trust that emerged in 1986, coinciding with the incorporation of Spain into the European Economic Community. To obtain the mark, certification is performed by an independent entity that controls an organisation which fulfils the requirements defined in standards or technical specifications. In addition, it must adhere to an arbitration system to solve possible disputes. Companies that obtain the certificate can incorporate the appropriate mark, certifying that the company has been registered in the Register of AENOR and complies with the requirements of the code of good practice.

**European Quality Assurance (EQA) promotes Internet Quality Assurance (IQA)**

The European Quality Assurance (EQA) promotes Internet Quality Assurance (IQA). It is a guarantee that ensures minimum requirements in e-commerce. It includes the certified quality of every step of the sale of products and services, whether they have a direct or indirect relationship with the customer. It also includes a management module that allows for the existence of internal procedures to ensure proper management.

### 3.7.5. SELECTED SECURITY CERTIFICATION BODIES AND THEIR WORK

#### 3.7.5.1. SELECTED PRIVATE CERTIFICATION BODIES

This sub-chapter provides information on two important providers of security certification in Spain: SGS and TÜV Rheinland.

**SGS**

<table>
<thead>
<tr>
<th>Kinds of PSS which are tested and certified in the security field</th>
</tr>
</thead>
<tbody>
<tr>
<td>SGS certifies products and systems in the security field (i.e. information security ISO 27001, airport safety, the classification and labelling system and Safety Data Sheets (SDS), CE marking...)</td>
</tr>
</tbody>
</table>

\(^{341}\) The Ethic Code is available on [http://www.autocontrol.es/pdfs/cod_confianzaonline.pdf](http://www.autocontrol.es/pdfs/cod_confianzaonline.pdf)

\(^{342}\) Further information can be found under: Eller Solutions, “Trusted Shops”, no date. [http://www.esellersolutions.com/partners-trusted-shops.html](http://www.esellersolutions.com/partners-trusted-shops.html)
Certification process(es) in the security area

SGS is a company that provides inspection, verification, testing and certification services and certifies based on ISO 17020: 2012 and ISO 17025: 2005. (ISO 17020 Conformity assessment standards. Requirements for the operation of various types of bodies performing inspection and the ISO 17025 standard on general requirements for the competence of testing and calibration laboratories do not refer to specific products or services but they regulate how CABs must develop the inspections (ISO 17020) or laboratory testing (ISO 17025)).

According to the ISO 17000:2004 standard on Conformity Assessment, all CABs (including SGS) must follow three steps: 1. Selection, 2. Determination and 3. Revision and attestation (meaning the latter as a declaration of verification), see below:

The certification process of any management system is based on this process, such as ISO 9001 or ISO 28000. Differences exist in particular regarding the particular requirements of each standard, e.g. concerning quality, security, environment, social responsibility etc.

The certification process of SGS is shown in the following figure.

[Diagram of certification process]

---

Documents which form the basis of the testing and certification process(es)

| Standards | ISO 9000 family standards, ISO 17000 family standards
| ICE family standards (CENELEC), ISO standards
| UNE standards (harmonized voluntarily or compulsory compliance)
| ASTM standards (harmonized standards from UE)
| ASME standards (standards form American Mechanical Engineers Society) |
| Internal guidelines/documents | Internal procedures that are the base to accredit parameters the organisation needs to certify
| Other documents | Procedures developed by Inspection and Certification Bodies Associations
| Security PSS which are certified based on the aforementioned standards | General criteria for accreditation from ENAC, CEA-ENAC and specific criteria for accreditation from ENAC, CEA-ENAC depending on each type of scheme. |
| Product/technology/system/service | Standard(s) used in the certification process
| Security PSS which are certified based on any other aforementioned documents (laws/regulation, internal guidelines/documents etc.) | -no specific information on security solutions available-

| Product/technology/system/service | Documents |
| Basically Industrial Facilities subject to regulations such as:
| Vehicles and containers.
| Construction of risky machines.
| Serious accidents. | Industry Law 21/1992 and its regulatory developments under the quality system of ISO 17000 standards are credited as fulfilling each specific installation developed by Royal Decrees. They can be complemented with specific regional decrees to each installation. |
### Quality seal

-no specific seal for security products-

Example for SGS seals in general (ISO 9001:2000):

![Quality Seal: ISO 9001:2000 (Source: SGS)](image)

### Key evaluation criteria in the security field and requirements for obtaining a certificate

No answer.

### Cooperation with external test laboratories in the security field

For intercomparisons of laboratory equipment according to ISO 17025 or external calibrations for measuring equipment. These are usually competitive. Anyone who is accredited in the field.

### Involvement of the organisation in security standardisation

Committees AEN/CT 192 on Regulatory Inspections and many others at the international level.

### Number of certificates issued in the security field annually

No answer.

### (Mutual recognition) agreements with other European countries/certification bodies in the security field

The National Accreditation Body has this kind of mutual recognition agreements. Conformity Assessment Bodies that are accredited under the ENAC mark can work in countries that have mutual recognition\(^{344}\).

### Solutions for suppliers of certified security solutions from other European countries that wish to receive a certificate that is valid in the country

These providers should talk to their National Accrediting Agency in order to try to reach an agreement with the Spanish Accreditation Body (ENAC).

---

\(^{344}\) Entidad Nacional de Acreditación, Los Acuerdos Multilaterales de Reconocimiento, no date.  
http://www.enac.es/web/enac/acuerdos_multilaterales_reconocimiento
TUV Rheinland

<table>
<thead>
<tr>
<th>Kinds of PSS which are tested and certified in the security field</th>
</tr>
</thead>
<tbody>
<tr>
<td>The services address in particular the supply chain as well as industrial security systems and equipment and shipments.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Certification process(es) in the security area</th>
</tr>
</thead>
<tbody>
<tr>
<td>TUV Rheinland is a certification and inspection body that provides services based on the following standards:</td>
</tr>
<tr>
<td>• Inspection and monitoring (ISO/IEC 17020: 2012).</td>
</tr>
<tr>
<td>• Certification of management (ISO/IEC 17021).</td>
</tr>
<tr>
<td>• Certification of products and services as well as testing of products: (EN 45011: 1998)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Documents which form the basis of the testing and certification process(es)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards</td>
</tr>
<tr>
<td>ISO/IEC 17020:2012</td>
</tr>
<tr>
<td>• Inspection and approvals of vehicles for export and import</td>
</tr>
<tr>
<td>• Inspections pre shipment and post shipment of products</td>
</tr>
<tr>
<td>• Notified Body for the implementation of European Directives for CE marking or other markings</td>
</tr>
<tr>
<td>ISO/IEC 17021:2011 and based on this standard:</td>
</tr>
<tr>
<td>• ISO 9001:2008</td>
</tr>
<tr>
<td>• ISO 28001:2007</td>
</tr>
<tr>
<td>• Other documents related to the supply chain such as TAPA (from the Transported Asset Protection Association); truck safety requirements (TSR) and safety requirements for cargo (FSR), C-TPAT Security Transport for Imports to the U.S.,</td>
</tr>
<tr>
<td>• ISO 27001 information security management</td>
</tr>
<tr>
<td>• ISO 20000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Laws/regulated</th>
</tr>
</thead>
<tbody>
<tr>
<td>National legislation on security and control as well as specific legislation for products and sectors</td>
</tr>
<tr>
<td>European legislation (new approach Directives)</td>
</tr>
<tr>
<td>Legislation applicable throughout different countries at an international level as well as legislation for access to markets.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Internal guidelines/documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>More than 2,000 documents and internal guidelines depending on the activity sector.</td>
</tr>
<tr>
<td>Regarding to Security PSS, there are specific guidelines/documents for each PSS certified.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>No answer.</td>
</tr>
<tr>
<td>Security products/technologies/systems/services which are certified based on the aforementioned standards</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>-no answer regarding security solutions-</td>
</tr>
</tbody>
</table>

**Quality seal**

A Hallmark unique quality seal by product, service, company with international database searchable via web and mobile devices using QR code page or by introducing the unique ID.

![Quality Seal (TUV Rheinland). Source: TUV Rheinland company](image)

**Key evaluation criteria in the security field and requirements for obtaining a certificate**

<table>
<thead>
<tr>
<th>Evaluation criterion</th>
<th>Minimum requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any of the services</td>
<td>The minimum required in the standard</td>
</tr>
</tbody>
</table>

**Cooperation with external test laboratories in the security field**

TUV Rheinland uses its own external accredited laboratories.

**Involvement of the organisation in security standardisation**

As an international organisation for inspection, testing and certification TUV Rheinland actively participates in standardisation committees and technical advisory groups in many countries.

**Number of certificates issued in the security field annually**

No answer
(Mutual recognition) agreements with other European countries/certification bodies in the security field

The agreements are set by international agreements of mutual recognition of the organisations that regulate these agreements (IAF, IFIA\textsuperscript{345}).

Solutions for suppliers of certified security solutions from other European countries that wish to receive a certificate that is valid in the country

TUV Rheinland is present in all continents and is a highly internationally recognised organisation by all governments with over 140 years of history now. It provides advanced service for access to international markets in compliance with all applicable regulatory and technical requirements.

3.7.5.2. Certification at the National Cryptologic Centre (CCN)

The National Cryptologic Centre (CCN) is a Certification Body (CB) of the Spanish Evaluation and Certification Scheme of information technologies, which apply to products and systems in this area. It operates under the Act 11/2002, 6th May that regulates the National Intelligence Centre (CNI).

The OC’s scope includes public or private entities who wish to function as evaluation laboratories for ICT security, as well as public or private entities manufacturers of ICT systems or products who wish to certify the security of these products or systems, as long as these products or systems can be included in the CCN’s scope.

The CCN offers three types of certifications, depending on the security features evaluated:

- Cryptology Certification: products capable of protecting national classified information.\textsuperscript{346}
- TEMPEST Certification: encryption equipment and ZONING evaluation.\textsuperscript{347}


\textsuperscript{346} The CCN is the Organization responsible for creating the Catalogue of Products with Cryptologic Certification that includes products capable of protecting national classified information. This way, the evaluated encryption equipment that obtains the CCN’s certification is considered as a national encryptor, and it obtains a cryptology certification. To obtain the certificate, the product must already have a Common Criteria certificate. The corresponding technical evaluation report is first delivered to the National Cryptologic Centre. Subsequently, the cryptology evaluation is carried out, during which the analysis of the encryption algorithms, security mechanisms and the proper functioning of the equipment is taken into account. The equipment is then assigned the maximum level of information classification for which it is authorized to handle. Every product with a cryptology certification has its own usage procedure which is mandatory to keep the authorisation to handle national classified information up to the maximum level of classification given to the product. The CCN policy on this matter is to increase the use of national encrypted equipment certified in Public Administration organisations.

\textsuperscript{347} The CCN is the authorised certification body for TEMPEST certification for the Ministry of Defence and as such, it is responsible for the development of regulations for the protection of equipments/systems that process and store classified information. As in other NATO member countries, the national regulations are designed to be compatible with those of the Alianza (Alliance). In some cases, these norms are extended to adapt to the needs of the Spanish Administration, especially in the evaluation of encryption equipments and risk assessment results that show undesired electromagnetic radiation in their facilities, this being the objective of the TEMPEST study. TEMPEST refers to investigations and studies on compromising emanations related to classified information which is being sent, received, managed or somehow processed by either electronic equipment or systems. Once detected and analysed, such unintentionally emanations can lead to the obtaining of information. TEMPEST also refers to the measures implemented regarding the protection against such compromising emanations. The CCN, as security certification authority for Information Technologies in EMSEC scope, has actively participated in the development of the Spanish TEMPEST regulation. The TEMPEST directive (CCN-STIC-210) is applicable to national...
• Functional certification: ITC products and systems evaluated, in accordance with international standard criteria (INTSEC and Common Criteria).

A. Functional certification. CB certifies the security of information technology products in accordance with the procedure established in the Fifth Title, and following the evaluation standards, criteria and methodology listed in the Sixth Title of the cited IT security evaluation and certification regulations.

Its certification is in accordance with the following international standard criteria:

• “Information Technology Security Evaluation Criteria” (ITSEC) and

The OC/CCN has been operating since 2004 with several evaluation standards for ICT security, including the Common Criteria (ISO-15408), which is the most internationally renowned. This standard is used for the certifications of products to be used in the Spanish eGovernment.348 This standard defines assessment levels between EAL7 and EAL1, being the CCRA international agreement the one that covers the mutual recognition of certificates between levels EAL1 to EAL4.

B. CNN accreditation to laboratories. The accreditation of such laboratories that perform the functional evaluation of the security of ICT products, under the scope of the Spanish Evaluation and Certification Scheme, is regulated by the following regulations:

• IT security evaluation and certification regulations, approved by Order PRE/2740/2007
• Accreditation of laboratories: Operative procedure PO-006; Act 21/1992, de 16th July, of Industry; Royal Decree 2200/1995, 28th December, by which the Regulation on Quality and Security Industrial Infrastructure is passed and
• Act 30/1992, de 26th November, on Juridical Regime of Spanish Public Bodies and of Common Administrative Procedure.

3.7.6. EXAMPLES FOR THE USE OF SECURITY STANDARDS FOR CERTIFICATION IN SPAIN

This section aims to present an overview of three multinational standards that have been adopted as national standards in Spain.

Airport and aviation security services (UNE-EN 16082)

The UNE-EN 16082 specifies the requirements and criteria for the quality of service for the organisation, processes, staff and management to be complied with service providers of classified information, either confidential or even more secret. Therefore, it covers equipment, systems and installations, fix and mobile alike, in which information is being generated and processed.

348 The Royal Decree 3/2010 of January 8, which regulates the National Security Framework – ENS – in the field of eGovernment, states in its article 18 that security products with the appropriate security certification will be positively valued for their acquisition by public administration. This certification should comply with international norms and standards, and the OC/CCN will determine the criteria to be followed, depending on the intended use of the product, on the evaluation level, and on other security certifications required by regulations.
airport security. It also establishes a methodology for the selection and recruitment of staff, establishing training as a key element, dealing with aspects related with security guards such as basic and specialized training of supervisors in the workplace (both initial and recycling). Certification is provided by the four organisations accredited by AESA.

**Alarm systems. Intrusion and hold-up systems. System requirements (UNE-EN 50131)**

The UNE-EN 50131 standard was originally published by CENELEC in 1997. However, this standard was not harmonized at national level due to the lack of additional regulations published to support it. It came into force on August 18, 2011 and it tries the design and installation of protection systems in the installation of intrusion alarm systems in order to adapt in the best way to the different types of installation.

All components must be assigned a security level, which must be printed on the product label or the supporting documentation. Thus, the overall level of an alarm system is the degree of the component with the lowest degree in the system. The grades are defined as detailed:

- **Grade 1**: low risk. It is expected that an intruder with no or little knowledge of an intruder alarm system.
- **Grade 2**: moderate risk. An intruder is expected to have a limited knowledge of an intruder alarm system.
- **Grade 3**: moderate to high risk. It is expected to be knowledgeable of the intruder alarm system intrusion.
- **Grade 4**: high risk. It is used when an attacker has the ability or resources to plan an intrusion in detail and has a full range of tools and equipment including replacements of components in a system intruder alarm.

Certification services are offered by AENOR.

**Ships and marine technology. Maritime port facility security assessments and security plan development (UNE-ISO 20858:2012)**

This international standard provides a framework for assessing the protection of maritime port facilities, developing security plans for these facilities, including corrective measures as well as the skills and knowledge required by the facility staff. It also contains requirements relating to documentation that is required in order to ensure that the process used to carry out these task have been collected so that an independent verification by a qualified and authorized body is permitted. It is designed to ensure that the completed tasks are in accordance with the requirements of IMO (International Maritime Organization), with the Code of International Ship and ISPS (International Ships and Port Facility Security Code) and the maritime security practices appropriate verified by an external auditor. Certification services are offered by AENOR.

### 3.7.7. Certification of drones

**Introduction**

This sub-chapter presents the current state of drone certification in Spain. Conform with current EU documents, this chapter uses the term ‘Remotely Piloted Aircraft Systems’ (RPAS) as a synonym for drones.
The Riga Declaration on Remotely Piloted Aircraft Systems (RPAS),\(^{349}\) held in March 2015 brought together the main representatives of the European aviation industry. The aim of the agreement was to get a consensus on a legislative framework for RPAs not beyond 2016. The main principles listed in Riga Declaration involve the necessity to establish a high level of security, safety and data protection requirements, and to clarify RPAS operators’ responsibility.\(^{350}\) However, while this European regulatory framework is being developed, countries are authorized to develop national measures and procedures to support limited RPAS with the necessary levels of security. At the moment, only a selected group of mostly European countries (including Spain) have developed and approved specific laws to regulate this activity. This regulation is trying to fill the legal gap within the sector, as it slows down its development for civil uses and prevents the exploitation of its great economic potential.

The Spanish legal framework for Remotely Piloted Civil Aircrafts

On 4 July 2014 the Spanish Government passed the Royal Decree-Law 8/2014 approving urgent growth, competitiveness and efficiency measures (RD 8/2014). Section 6 of the Royal Decree adopted the temporary legislative measures for remotely piloted civil aircrafts (RPA), the so-called drones, weighing less than 150 kilos in order to carry out technical or scientific work or more than 150 kilos only intended for fire-fighting and search and rescue activities. The Royal Decree has been transformed into Law 18/2014, 15 October 2014.\(^ {351}\) This norm has temporary validity until “the Government will determine the legal regime applicable to remotely-piloted civil aircrafts as well as operations and activities undertaken by them. When the new norm entries into force, the regulatory provision will be ineffective” (Second final provision paragraph 2 of Law 18/2014). At the time of the approval of RD 8/2014, Spain was “presented as one of the pioneering countries in regulating the activity of these aircrafts pre-empting Europe Union –including the vast majority of EU Member States, except in the case of France, where it was regulated in 2012-- as well as the Unites States of America –where the Federal Aviation Administration is still starting to approach this issue--”.\(^ {352}\)

---


350 As EUROCONTROL states minimum principles to integrate RPAS into the present aviation environment have already been agreed at an international level: 1. They should not pose an additional hazard to existing operations, 2. They should be as safe as or safer than manned aircraft operations and 3. They should operate in a transparent manner for ATC. On its part, the key principles of the Riga Declaration can be summarized as follows: Drones need to be treated as new types of aircraft with proportionate rules based on the risk of each operation (i.e. the use of drones cannot be less safe than is accepted from civil aviation in general, although the way safety is regulated must be proportional to the operational risk involved); EU rules for the safe provision of drone services need to be developed now (and the essential requirements should be harmonized at the global level to the maximum extent possible), Technologies and standards need to be developed for the full integration of drones in the European airspace, Public acceptance is key to the growth of drone services (that is, preventing the malicious use of drones and guaranteeing the respect of citizens’ fundamental rights, the right to privacy and the protection of personal data), The operator of a drone is responsible for its use (accountability and third-party liability are necessary to compensate for potential victims or harms) and, finally, The development of drone services and drone technologies needs close monitoring to ensure that new technologies and drone services can develop in full respect of the required high levels of safety, security, privacy and environmental protection.

351 Section 86 of the Spanish Constitution states that “1. In case of extraordinary and urgent need, the Government may issue temporary legislative provisions which shall take the form of decree-laws (...). 2. Decree-laws must be immediately submitted for debate and voting by the entire Congress, which must be summoned for this purpose if not already in session, within thirty days of their promulgation. The Congress shall adopt a specific decision on their ratification or repeal in the said period (...).”

Despite the popular expression “drones”, the Spanish Law follows the recommendations of the European Economic and Social Committee and it uses the term preferred in Europe and by ICAO, that is to say, a literal translation of the real name for this new type of airspace user “Remotely Piloted Civil Aircraft” (Aeronaves civiles pilotadas por control remoto, in Spanish). 353

Law 18/2014 primarily seeks to clarify the definition and classification of RPAs, followed by a classification of drones limitations and requirements depending on their weight. Then it focuses on the necessary training for pilots of unmanned aircraft, certificates and examinations as well as limitations and possible applications. This Act ends by explaining the future provisions for this type of aircraft. The law deals exclusively with the operation of RPA less than 150 kilos (or more than 150 kilos intended for fire-fighting and search and rescue activities).

- The Spanish regulation allows the use of drones for aerial activities such as: research and development activities; aerial treatments, pesticides and other treatments involving spreading substances in the soil or atmosphere, including activities for firefighting; observation and aerial surveillance activities including filming and monitoring of forest fires; aerial advertising, radio and TV emissions and emergency, search and rescue operations as well as other special works.

- Aerial activities for the purpose of technical or scientific work carried out by RPA may be performed in daylight and in visual meteorological conditions and in all cases in zones away from built-up areas in towns, villages or inhabited places, and away from open-air assemblies of persons (Section 50.4).

- Provisions in Law 18/2014 have to be completed with some extra legislation applicable to operators, in particular with regard to use of the radio spectrum, data protection or the taking of aerial photographs, nor from his/her liability for any loss, damage or injury caused by the operation of the aircraft (Section 50.1).

- RPA having a maximum take-off weight of more than 25 kilos shall be entered in the aircraft register and have an airworthiness certificate. RPA having a maximum take-off weight equal to or less than 25 kilos shall be exempt from these requirements (Section 50.2).

- Regardless of weight, there are some common requirements for all types of aircrafts.
  - All RPA shall have affixed to their structure an identification plate, indicating in clearly legible and indelible form the identification of the aircraft, by means of the specific designation and, where applicable, a serial number, and the name of the operating company and the information required in order to contact it.
  - The operators must have an available operational manual (i.e. criteria for determining the take-off and landing areas, analysis of the weather conditions, fuel or energy management, etc.), an aeronautical safety study for each operation, the perceptive documentation on the characteristics of the aircraft, a programme of

353 Recommendation 2 of the EESC Opinion on Remotely Piloted Aircraft System of 15 October 2014: “The terms RPAS and UAV (unmanned aerial vehicle) follow the international regulations set by the International Civil Aviation Organization (ICAO). ICAO does not use the description "drone", but it is now firmly established in popular parlance. In order to avoid legal confusion, including as regards liability and insurance, it would nonetheless be advisable to work towards using the ICAO terminology in the European context". As David Wright clarifies “Aficionados, especially industry and policy-makers don’t much like the word (drone). Aficionados prefer more bureaucratic terms, like unmanned aerial vehicle (UAV) or unmanned aerial system (UAS), which are the preferred terms in the US, or remotely piloted aircraft system (RPAS), the term preferred in Europe (and by ICAO)” (D. Wright, “Drones: Regulatory challenges to an incipient industry”, Computer Law & Security Review, num. 30, 2014, p. 226.
maintenance of the aircraft according to the manufacturer’s recommendations, a pilot who meets the legal requirements and a flight insurance under current regulations. Appropriate measures must be taken to protect the aircraft from unlawful interference during operations, to ensure the safety of the operation and to protect persons and property overflown. Operations must be carried out at a distance of at least 8 km from any airport or aerodrome (if the drone is less than 2 kilos, at a minimum distance of 15 km from its reference point).

- The Law establishes requirements on the maximum takeoff weight of the apparatus and classifies aircraft of more than 25 kilos, less than 2 kilos and up to 25 kilos (Section 50.3).\(^{354}\)

The following figure summarizes the results.

<table>
<thead>
<tr>
<th>Type of drone</th>
<th>&lt; 2 kg</th>
<th>≤ 25 kg</th>
<th>+ 25 kg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visual range</td>
<td>Radio control station</td>
<td>Visual range of the pilot</td>
<td>Depending on airworthiness certificate</td>
</tr>
<tr>
<td>Maximum distance</td>
<td>Control station</td>
<td>500 meters (1,670 feet)</td>
<td>Depending on airworthiness certificate</td>
</tr>
<tr>
<td>Maximum height</td>
<td>120 meters (400 feet)</td>
<td>120 meters (400 feet)</td>
<td>Depending on airworthiness certificate</td>
</tr>
<tr>
<td>Identification</td>
<td>License plate</td>
<td>License plate</td>
<td>License plate + Identification of the aircraft</td>
</tr>
<tr>
<td>Authorization</td>
<td>Notification (5 days prior to commencement of the operation)</td>
<td>Liability statement</td>
<td>Airworthiness certificate + Aircrafts Registry</td>
</tr>
</tbody>
</table>

Source: AESA
Figure 47: Principles for the certification of drones in Spain

\(^{354}\) The rules of usage of those aircrafts not falling under those categories would be subjected to European Union regulation.
More information is given in Annex of chapter 3.7.

Registration of drones operators in Spain

As described earlier AESA is the state body that ensures that civil aviation standards are observed in all aeronautical activity in Spain. Regarding RPAS, AESA is active ensuring that RPAS operations are supported and regulated in Spain and is competent for:

- Management of the Aircraft Registration Records,
- Issuing of the type certificates for ultralight motorized aircrafts,
- Approving training organisations (ATOs),
- Issuing the certificate of airworthiness for any type of remote piloted aircrafts,
- Issuing the specific permission for RPAS under 25 kilos (an acknowledgment of receipt),
- Issuing authorization for RPAS over 25 kilos.

As we have seen, the Spanish legislation states that operators of drones under 25 kilos do not need a permission from AESA but they must submit to the Agency a responsible statement where they confirm to meet all the requirements set by law. The operators of drones over 25 kilos are obliged to request authorization to the Agency to operate this type of aircraft, and, so far, there are two operators who have requested such authorization. The documents to be presented by an operator willing to fly an RPAS over 25 kilos are the following:

- Documentation on the characteristics of the aircraft (configuration, features and capabilities)
- Operational Manual (Section 50.3.d.1)
- Aeronautical safety study for each operation
- Test flights that are necessary to demonstrate that the intended operation can be performed safely (Section 50.3.d.4 and 50.6)
- Program of maintenance of the aircraft according to the manufacturer’s recommendations (Section 50.3.d.5 and 50.6)
- A pilot who meets the legal requirements (a) Theory knowledge: to pass a course in an ATO (b) practical knowledge: provided by operator
- Flight insurance under current regulations.

---

356 Document in AESA, Apéndice E, Contenido del Manual de Operaciones (art. 50.3.d.1°) http://www.seguridadaerea.gob.es/media/4243290/140707_apendice_e.pdf
357 Document in AESA, Apéndice F, Estudio Aeronáutico de Seguridad en la Operación de Aeronaves Pilotadas Por Control Remoto (art.50.3.d.3°, 50.4 y 50.6) http://www.seguridadaerea.gob.es/media/4243042/140707apendice_f.pdf
358 Document in AESA, Apéndice G, Contenido de “los vuelos de prueba que resulten necesarios para demostrar que la operación pretendida puede realizarse con seguridad” (art. 50.3.d.4 y 50.6) http://www.seguridadaerea.gob.es/media/4243046/140707_apendice_g.pdf
359 Document in AESA, Apéndice H, Revisiones y Pruebas a Incluir en el Programa de Mantenimiento de una Aeronave Pilotada por Control Remoto (art. 50, 3.d.5 y 50.6) http://www.seguridadaerea.gob.es/media/4243050/140703_apendice_h.pdf.

The legal conditions will be described in the next chapter.

**Legal conditions and requirements for drone pilots**

All drone pilots, regardless of the size of the aircraft, must comply with several requirements (Section 50.5):

• They have to provide conclusive proof that they have the theoretical knowledge required to obtain a pilot’s license which can be achieved by three means
  - Hold or have held (in the last five years) a pilot’s license (of any kind, including an ultralight pilot’s license),
  - Provide conclusive proof of having the theoretical knowledge to obtain the license (by a certificate of knowledge issued by a training organisation approved by EASA (approved training organisation, ATO) or, in case of having knowledge for an ultralight pilot’s license, by an individual certificate after the correspondent examination)
  - In the case of an aircraft under 25 kilos by a basic certificate issued by an ATO after successfully having passed a course.
  - In case of not having a pilot’s license, they must be eighteen years old.

• They have to hold a medical certificate for the light aircraft pilot license (class LAPL for aircrafts under 25 kilos) or a medical certificate by an authorized aero-medical examiner or aero-medical center (class 2 for aircrafts over 25 kilos).

• In addition, they must also have a document proving that they have sufficient knowledge of the aircraft and its systems, and of how to pilot it, which has been issued by the operator, by the manufacturer of the aircraft or a training organisation authorized by the manufacturer, or by an approved training organisation.

Pilots must always be authorized to be able to fly the drones. Although drone flights aren’t allowed over built-up areas, flights in fully enclosed areas aren’t subjected to AESA jurisdiction. In these cases, the owners of the closed areas are responsible for the correspondent authorization for the flight.

Many people are obtaining their certificate in an approved training organisation and this option is one of the most required in Spain.\(^{360}\) Section 50.5 of the Law establishes the requirements to issue a “basic certificate” or an “advanced certificate” for operating a RPA. The organisation will be “a training organisation approved in accordance with Annex VII to Regulation (EU) nº 1178/2011 of the Commission of 3 November 2011 laying down technical requirements and administrative procedures related to staff flight of civil aviation”. Therefore,

\(^{360}\) The list of approved training organisations in Spain, dated on 6 March 2015, has around 100 organisations: Ministerio de Fomento, Listado de Organizaciones de Formación Aprobadas ATOs, Madrid 06.03.2015. http://www.seguridadaerea.gob.es/media/4201412/atos.pdf
the training organisation must obtain approval from EASA under the abovementioned Regulation of the European Commission.

Finally, the use of drones involves serious conflicts in the area of privacy of citizens; especially if applied in the field of security and surveillance. Law 8/2014 stresses the operator’s responsibility for damage or injured caused while operating a drone or by the aircraft itself, as well as the obligation to comply with the legislation on data protection or the one applicable to the capturing of aerial images. It is quite common that these aircrafts are fitted with a camera which may capture – and store - images of people. Undoubtedly, the use of drones for aerial photography when images of persons can lead to identification, fall under the scope of the data protection law and rights to privacy and to data protection have already been addressed in European legislation and even in national constitutions. RPAS will not be exempted from these rules.\(^361\)

In general terms, the Spanish Data Protection Law 15/1999 of 13 December (LOPD) embodies the principles of transparency, data minimization, proportionality, legitimate purpose for the treatment, consent, accountability, data security, rights of access, correction and erasure and third country transfers. Regarding activities carried out by drones in public services, the applicable legislation is the Law 4/1997 of 4 August, approving the use of video cameras by the Security Forces in public places and the implementing regulations (Royal Decree 596/1999, of 16 April). Apart from these regulations, companies in the sector must pay attention to the decisions and guidelines given by the Spanish Data Protection Agency on this matter. Operators and pilots must regulate, depending on the mission and the context, the strategy to be followed to ensure an adequate policy of protection of personal data. In this regard, one of the most used methodologies to mitigate the impact on personal data is conducting Privacy Impact Assessment (PIA). A Privacy Impact Assessment Guide was published by the Spanish Protection Agency (AEPD) in 2014. The Guide defines in detail the steps to be followed to conduct a PIA and indicates some situations where it would be advisable to conduct this analysis: “when technologies are considered highly invasive to privacy, such as large-scale video surveillance, the use of unmanned aircrafts (drones) … (and) geolocation…”\(^362\)

**Current activities in the industry**

Several requirements have been established by AESA regarding the practical training for pilots. A manufacturer is only authorized to provide practical training for their own aircrafts. This practical training must meet the minimum requirements established in Appendix I of Acceptable Means to Prove Compliance Requirements for Pilots for Remote Piloted Aircrafts (Section 50.3 of Law 18/2014)\(^363\). The first certification of airworthiness provided by AESA was in 19 February 2010 for a test flight. Regarding certification entities, the most representatives’ ones in Spain are the following.

The National Institute of Aerospace (INTA) is the public research organisation specialized in aerospace research and technology development. Among its main functions it is worth men-

---


tioning performing all types of tests to check, approve and certify materials, components, equipment items, subsystems and systems that have an aerospace application. INTA performs activities for RPAS in their laboratories, i.e., environmental testing or electromagnetic compatibility tests.

EuroUSC™ is a qualified entity who covers the accreditation of Operators, Manufacturers and Flight Training Schools involved in light UAS which require permissions or exemptions to operate within the national context, as defined by the appropriate National Aviation Authority (NAA). EuroUSC opened its office in Madrid in 2013 to assist the process of ensuring that Spanish industry has a safe and expedient way to grow in line with AESA’s regulatory determination. BNUC-S™ Part 1 Ground School Course enables Spanish organisations wishing to operate in all countries that accept the BNUC-S™ standard to undertake VLOS Operations. It is expected that AESA may accept recommendations from EuroUSC™ on a case by case basis as its regulatory framework for RPAS operations evolves. It is expected that AESA may accept recommendations from EuroUSC™ on a case by case basis as its regulatory framework for RPAS operations evolves.

Alter Technology offers a new service as a certification entity for the EGNOS Enabled Label, which guarantees that products use EGNOS (European Geostationary Navigation Overlay Service) in their positioning and timing services. This assures business partners and users that EGNOS Open Service features are implemented. The label can be obtained by manufacturers of receivers and of GNSS (Global Navigation Satellite System) enabled devices. The certification procedure is based on a technical verification process. Specific tests on the product and its reactions to adverse or demanding conditions will prove that it uses the information provided by EGNOS. Based on the tests, five different levels are assigned for start-up time, accuracy and robustness. Once the label is granted, it can be communicated to the final consumers through a specific sticker on the product’s packaging. ALTER Technology is the first certification body to provide such service.

Annex: normative documents on drones

(Section 50.1 of Law 18/2014)


Royal Decree 1398/1993 of 4 August 1993 approving the Regulation on the Procedure for the Sanctioning Power


Law 48/1960 of 21 July 1960 governing air navigation

Royal Decree 57/2002 of 18 January 2002, for the regulation of Aerial Circulation

Law 21/2003 of 7 July 2003 governing air safety

Royal Decree-Law 98/2009 of 6 February 2009 laying down the Regulation of Aeronautic Inspection

Regulation (EU) n° 1178/2011, laying down technical requirements and administrative procedures related to civil aviation aircrew pursuant to Regulation (EC) n° 216/2008 of the Europe-
3.7.8. SUMMARY AND CONCLUSION

The Spanish security certification landscape consists of numerous players. The national standards developing organisation (SDO) AENOR is responsible for security standardisation and certification and could become an important partner for promoting European security certification solutions in the future. TEMPEST certification addresses issues related to the management of classified information via electronic methods and is strongly supported by EU authorities, making it an essential body to further examine. The German, globally operating service provider TUV Rheinland, which is also an active player in Spain, works to maintain a policy of global access via the development of new markets through the international certification of products with a focus on the international agreement “Global System for Conformity
Testing and Certification of Electrical Equipment", or IECEE, consequently promoting global harmonisation and reducing trade barriers by allowing for quick and easy access to major markets and simplifying the licensing and certification process. Many security-related CABs and PSS are already certified in Spain. The country is further working to eliminate technical barriers by fostering the role of external, independent and impartial accredited entities, although it is interpreted in a more flexible way as responsible statements.\footnote{It is a document signed by the owner of the business or its representative, which states, under its responsibility, he complies with certain requirements. However, these statements are not controlled by an independent third party and subsequently, they do not guarantee the access to international markets.}

3.7.9. REFERENCES


European Commission, Communication from the Commission to the European Parliament and the Council, 8 April 2014, *A new era for aviation - Opening the aviation market to the civil


3.7.10. Annex

Certification and technical instructions and guides for Airports

Certification
- CERA-09-GUI-001-2.0: Guide for the development of the Manual of Airport
- CERA-09-GUI-002-1.0: Guidelines for presentation of opinionicultural compliance with technical standards
- CERA-09-GUI-003-1.0: Guide for the Development of Security Studies - Exemptions
- CERA-12-GUI-042-1.0: Guide for the development of SGS airport

Technical instructions and guides
Applicable for both certified and non-certified airports.
- CERA-12-GUI-034-1.0: Technical Guide for the Development of Security Studies in the field of SMS
- CERA-13-GUI-051-1.0: Guide for the development of studies of wildlife and their habitats in airport environments
- CERA-13-GUI-052-2.0: Guide for the development of risk assessments of impact wildlife at airports
- CERA-14-INS-019-1.0: General Technical Instruction for change management at airports
- INSA-11-INS-004-1.0: Technical Instruction on Training for rescue and fire fighting
- INSA-11-INS-005-1.1: Technical instruction on security requirements in service ground handling
- INSA-11-INS-006-1.1: Technical Instructions for the completion of an action plan to adverse weather conditions
- INSA-11-INS-007-1.1: Technical Instructions for the evaluation of the coefficient of friction of the surface of the track

Regulatory framework for Air Navigation

- Regulation of ATS provision, obligations of civil ATS providers and certain working conditions for ATCOs
  - Law 21/2003, of 7 July, that regulate the technical investigation of civil aviation accidents and incidents and establish the legal system for aeronautical inspection, the obligations related to air security and the system of offences and penalties in civil aviation matters
  - Law 9/2010, of April 14th, that regulates the provision of air traffic services, establishes the obligations of the civil providers of such services and lays down certain working conditions for the civil air traffic controllers.
- Modernization of airport management and issues related
  - Royal Decree-Law 13/2010 of December 3th, acting in fiscal, workrelated and liberalizing fields to promote investment and creation of employment.
- Certification of Air Navigation Service Providers (ANSPs)
  - Royal Decree FOM/931/2010, of 23 July, by which it is regulated the procedure for the certification of air navigation service providers and their regulatory oversight.
- Regulation of AFIS provision
  - Royal Decree 1133/2010, of September 10th, by which the provision of the Aerodrome Flight Information Service (AFIS) is regulated.
• Certification of ATCOs Training Providers
  – Order FOM/1841/2010, of July 5th, by which the requirements for the certification of air traffic controllers training providers are developed.

• Security standards in relation to ATC activity and rest requirements for civil Air Traffic Control Officers (ATCOs).
  – Royal Decree 1001/2010, of August 5th laying down aviation security standards in relation to ATC activity and rest requirements of the civil ATCOs.

• Modification of authorization and certification requirements for aerodromes
  – Royal Decree 1189/2011, of August 19th, regulating the procedure for issuing reports previous to the planning of aeronautical infrastructures and to the construction, modification and opening of aerodromes of competence of the Self Governing Communities; amending the Royal Decree 862/2009, of May 14th, approving technical standards for design and operation of public use aerodromes and regulates the certification of State competence airports; amending the Royal Decree 584/1972, of February 24th of aeronautical easements (aerodrome protection); and amending the Royal Decree 2591/1998, of December 4th regulating Master Plans and services areas of airports of general interest, as provided by article 166 of Law 13/1996 on December 30th of fiscal, administrative and social order measures.

• Apron Management Service, a service provided to regulate the activities and the movement of aircraft and vehicles on an apron.
  – Royal Decree 1238/2011, of September 8th, regulating the apron management service of the airport.
3.8. Sweden

3.8.1. Short description of Sweden’s security industry

Sweden has an advanced security industry. The total turnover of security and defence-related sales amounted to approximately SEK 30 bn (€ 32 bn) in 2013. Detailed information is provided by the Swedish Security and Defence Industry Association (SOFF). SOFF was founded in 1986 and comprises companies which develop and/or produce equipment and services, both military and commercial, for defence or civil security. The Association currently has approximately 60 member companies of which most are SMEs. SOFF’s perception of the market is described as follows:

“[N]ew and more unforeseeable risks such as regional and ethnic conflicts, natural disasters, organized crime, pandemics, climate change and different types of terrorist actions are (also) at the centre of attention.”

Civil security and dual-use products have steadily increased as shares of total sales for the Swedish security and defence industry (currently 35%). In part, this reflects the changing nature of the security environment since the terrorist attacks in the United States on 11th September 2001. In order to reduce the challenges associated with decreasing defence expenditures in Europe, several companies have deliberately broadened their product portfolio in order to expand market shares within the civilian security sector.

The Swedish Civil Contingencies Agency (MSB) coordinates and develops the preparedness of the Swedish society to manage serious crises. It works together with many partners, such as municipalities, county councils, government authorities and the business community. Currently, its main security priorities include: “technical infrastructure; transport; hazardous substances (including chemical, biological, radiological, nuclear); economic security; coordination and information by geographical area; protection, emergency response and care”.

The most important market segments are ‘equipment for both domestic and corporate security and protection, ranging from simple alarms and protective devices to complex wireless digital systems that integrate fire alarm, passage control, area control and CCTV. Other growing sectors are consultancy and guard services and security training sectors. In the IT security market the largest subgroups are identification systems, antivirus programs, Public Key Infrastructure (PKI), intrusion detection and backup equipment.”

The turnover of the private security service providers was € 840 million in 2010. This number builds upon the following segments: General guarding (excluding the segments listed hereafter): € 525 million, airport security: € 52.5 million, maritime security: € 10.5 million,

366 SOFF, op. cit., 2013, p. 12
371 Confederation of European Security Services (CoESS), op. cit., 2011.
3.8.2. The Security Standardisation Framework

Sweden’s national standards body is the Swedish Standards Institute (SIS). In addition, the Sveriges Standardiseringsförbund (Swedish Standards Council) at SIS is the principal body for all Swedish standardisation activities. Sveriges Standardiseringsförbund is tasked with promoting interest in standardisation and the employment of standards. The Swedish State and Svenskt Näringsliv (the Confederation of Swedish Enterprise) appoints Sveriges Standardiseringsförbund commissioners. Based on CRISP’s interests in the security field, the work of twelve SIS TCs was analysed.

• TC 166 Packaging logistics and traceability.
• TC 172 Secure storage of cash, valuables and data media
• TC 255 Intelligent transport systems
• TC 303 Systems and software engineering
• TC 318 Information security management systems
• TC 334 IT applications in health care technology
• TC 360 Protection against fire
• TC 448 Identification cards
• TC 451 Financial systems
• TC 494 Societal security
• TC 578 Maritime and port security services
• TC 585 Private security companies

The TCs were analysed in detail with the following results:

TCs 318, 334, 578 and 585 are only involved in European and/or international standardisation work. TC 255 works on national projects but not in the security field. In contrast, the following TCs have been active in national security-related projects:

TC 166 developed only one national standard: SS 30805 Data representation - Character Set OCR-B - Shapes and dimensions of the printed image.

Based on an analysis with the additional keyword “cert”, one nationally focused document of TC 172 could be identified: SS 3880, Högsäkerhetslås - Krav och provning.

TC 303 also created a number of national documents, but most of them address information technology.

TC 360 has created six documents with a specific national focus.

• SIS-TR 47:2014, Brand och räddning - Signalkarakterärs för brand- och utrymningslarm
• N 748, Inductionsproportioner PN 16 for foam compounds
• SS 3654, Brand och räddning - Branddetekterings- och brandlarmssystem - Brandförsvarsvarstablå och brandkårsnyckel
D2.2: Consolidated report on security standards and certification

- SS 883001, Brand och räddning - Boendesprinkler - Utförande, installation och underhåll
- SS 883003, Brand och räddning - Boendesprinkler - Del 3: Vattendimystem likvärdigt med boendesprinkler
- SS 883007, Brand och Räddning - Brandgasventilatorer - service och underhåll för brandgasventilation

TC 448 is responsible for three national standards:

- (no number) Personal identification - Biometric application profiles for law enforcement and border control authorities using portable identification systems
- (no number) Environmental influence testing methodology for operational deployments of European ABC systems
- SS 614314, Identifieringskort - Certifierade identitetskort av typ ID-1

TC 451 created only one national standard: SS 38414 Notation of monetary amounts and currency designations. Finally, TC 494 is active in two specific fields on the national level:

- CBRN - ETE, CBRN - Education, training and exercises (ETE)
- CBRN, CBRN - Risk assessment, risk awareness and risk management

The following figure shows Sweden’s activities in selected ISO/IEC committees.

<table>
<thead>
<tr>
<th>ISO TC</th>
<th>Topic</th>
<th>Participation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC/JTC 1/SC 17</td>
<td>Cards and personal identification</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 27</td>
<td>IT Security techniques</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC JTC 1/SC 31</td>
<td>Automatic identification and data capture techniques</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 37</td>
<td>Biometrics</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 68</td>
<td>Financial services</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 85</td>
<td>Nuclear energy, nuclear technologies, and radiological protection</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 92</td>
<td>Fire safety</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 223</td>
<td>Societal security</td>
<td>P, Secretary</td>
</tr>
<tr>
<td>ISO/TC 224</td>
<td>Service activities relating to drinking water supply systems and wastewater systems - Quality criteria of the service and performance indicators</td>
<td>O</td>
</tr>
<tr>
<td>ISO/TC 247</td>
<td>Fraud countermeasures and controls</td>
<td>O</td>
</tr>
<tr>
<td>ISO/PC 284</td>
<td>Management system for quality of private security company (PSC) operations - Requirements with guidance</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 292</td>
<td>Security</td>
<td>P, Secretary</td>
</tr>
<tr>
<td>Total P+O</td>
<td></td>
<td>10+2</td>
</tr>
</tbody>
</table>

Source: Own analyses

Figure 48: Sweden’s involvement in selected ISO/IEC TCs
3.8.3. The Security Conformity Assessment Framework

The database of SWEDAC, the Swedish Board for Accreditation and Conformity Assessment, lists four certification and inspection bodies based on the search combination “security certification”: Intertek Certification AB, DNV GL Business Assurance Sweden AB, Försvarets Materielverk and SIS Förlag AB. All certification bodies are described in the next sub-chapter. The use of the search word ‘security’ alone unveils three additional players: atsec information security AB, Combitech AB and Svensk Brand- och Säkerhetscertifiering AB (SBSC). These organisations are more focused on safety-related certifications but also deal with security-related aspects. Based on searches for selected ISO and EN standards, SP Sveriges Tekniska Forskningsinstitut could be identified as an additional CAB. SWEDAC offers a map, which visualizes the country’s security certification infrastructure on its website (see Figure 49). In addition to the CABs accredited by SWEDAC, there are a few others, which are subsidiaries of foreign, multinational CABs.

![Swedish landscape of security certification and inspection services](image)

Source: SWEDAC
Figure 49: Swedish landscape of security certification and inspection services

According to the figure, there are three centres in Stockholm, Kista and Danderyd, but several services are offered in Solna, too. Additional CABs could be identified by the international website standards.org. The following figure gives an overview. More information will be provided in the next sub-chapter. Although there are several CABs in the security sector, many European and international security standards are currently not integrated in Sweden’s certification landscape (see Figure 51).
<table>
<thead>
<tr>
<th>Organisation</th>
<th>What is certified?</th>
<th>Basis of the testing and certification processes</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combitech AB</td>
<td>IT security</td>
<td>Common Criteria, SS-EN ISO/IEC 17025</td>
<td><a href="http://www.combitech.se/Om-Combitech/Foretagsfakta/">http://www.combitech.se/Om-Combitech/Foretagsfakta/</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The-Swedish-Certification-Body-for-IT-Security/</td>
</tr>
<tr>
<td>Intertek Certification AB</td>
<td>Information security management systems</td>
<td>ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems – Re-</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>quirements.</td>
<td><a href="http://www.intertek.se/">http://www.intertek.se/</a></td>
</tr>
<tr>
<td>Svensk Brand- och Säkerhetscertifiering AB (SBSC)</td>
<td>Safes, bars, locks, persons</td>
<td>e.g. SBF 1007-4</td>
<td><a href="http://www.sbsc.se/">www.sbsc.se/</a></td>
</tr>
<tr>
<td>SP Sveriges Tekniska Forskningsinstitut</td>
<td>Products, construction products, resistance to burglary, fire safety solutions</td>
<td>e.g. EN 5013 series, EN 54 series</td>
<td><a href="http://www.sp.se/en/Sidor/default.aspx">http://www.sp.se/en/Sidor/default.aspx</a></td>
</tr>
<tr>
<td>UL Verification Services</td>
<td>In particular transaction security services</td>
<td>div., e.g. ISO 7816 and 10373, C-TAP</td>
<td><a href="http://sweden.ul.com/">http://sweden.ul.com/</a></td>
</tr>
<tr>
<td>LRQA</td>
<td>Processes</td>
<td>ISO 28000</td>
<td><a href="http://www.lrqa.se/">http://www.lrqa.se/</a></td>
</tr>
</tbody>
</table>

Figure 50: Overview of Swedish CABs in the security field
<table>
<thead>
<tr>
<th>Standard</th>
<th>Accredited CABs</th>
<th>Names of the CABs</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 2800x, ISO/IEC 27000, IEC 62443, IEC 62642, EN ISO 22301, EN ISO 27799, EN 13094, EN 14025, EN 12972, EN 14339, EN 14384</td>
<td>--</td>
<td>-</td>
</tr>
<tr>
<td>EN 50131</td>
<td>1</td>
<td>SP Sveriges Tekniska Forskningsinstitut</td>
</tr>
<tr>
<td>EN 50133</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>EN 50136</td>
<td>1</td>
<td>SP Sveriges Tekniska Forskningsinstitut</td>
</tr>
<tr>
<td>EN 50518</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>EN 54 series</td>
<td>1</td>
<td>SP Sveriges Tekniska Forskningsinstitut</td>
</tr>
<tr>
<td>EN 62676</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Source: Own figure, SWEDAC
Figure 51: Selected standards as a basis for certification in Sweden

In addition to the CABs shown in Figure 50 and Figure 51, Inspecta Nuclear AB and TÜV NORD Sweden AB are responsible for issues of nuclear power. Furthermore, the Rikspolisistyrelsen is accredited for calibration, chemical analysis, flexible scope, scene investigation and forensic analysis (drug analysis, fingerprint), while ‘forensic analysis’ is also an area, in which Rättsmedicinalverket conducts accredited investigations. An additional important CAB in the public sector is FOI, which is the largest combined defence and national security research organisation in Sweden. FOI hosts one of the few security classified CBRN laboratories in Europe that is licensed to receive and examine all types of hazardous substances. Its scope also includes the measurement of and protection against the emission of CBRN substances. In the following chapter specific CABs and their work are described in detail.

---

372 SWEDAC’s database shows DNV GL Business Assurance Sweden AB as a second hit for the search term EN 54 but according to DNV’s profile on SWEDAC’s website (see http://search.swedac.se/en/accreditations/1053) the number 54 does not refer to an EN standard
373 SWEDAC, SWEDAC’s Database on accredited bodies, Nuclear Power, no date. http://search.swedac.se/en/accreditations?mode3_accarea_l1=Nuclear+power&mode3_accarea_l2=&mode3_accstd=&mode3_docs=
375 SWEDAC, SWEDAC’s Database on accredited bodies, Forensic analysis, no date. http://search.swedac.se/en/accreditations?mode3_accarea_l1=Forensic+analysis&mode3_accarea_l2=&mode3_accstd=&mode3_docs=
3.8.4.  SELECTED SECURITY CERTIFICATION BODIES AND THEIR WORK

3.8.4.1.  PRIVATE CERTIFICATION BODIES

This section describes the activities of nine certification bodies, which are important for Sweden’s security landscape.

SP Sveriges Tekniska Forskningsinstitut

Via its unit SP Certification, Sveriges Tekniska Forskningsinstitut is one of the leading bodies in the field of certification in Sweden. It issues certificates of compliance with a large number of standards for management systems, products, construction products and persons and is also Notified Body for a number of EU directives.⁴³⁷

Of particular interest is that SP is accredited for the certification of control units for cash registers. It describes the relevant services as follows:

“In Sweden, most businesses that sell goods or services for payment in cash are required to use an approved cash register, according to the Swedish Tax Agency’s regulations. The aim is to protect serious business within cash trade against unfair competition. The cash register shall be connected to a certified control unit. This control unit processes incoming data from the cash register and generates control data.”³⁷⁹

SP’s services also include certification based on the EN 5013x series, EN 50518 and the EN 54 series.³⁸⁰ In the field of safety, it certifies, for example, Fire resistant cabinets, tents, ladders, fire extinguishing foams and archival materials.³⁸¹

DNV GL Business Assurance Sweden AB

DNV GL Business Assurance Sweden AB belongs to the international organisation DNV GL, which was introduced in the German country study. Its security certification services are offered in Solna. Relevant accreditation fields include the certification of management systems and SS-ISO/IEC 27006:2007. Normative documents and related regulations are described below:

A) Information security management systems

Relevant regulations include:

⁴³⁹ Own analysis in SWEDAC database
D2.2: Consolidated report on security standards and certification

- STAFS 2010:10 SWEDAC’s Regulations and General Guidelines on Accreditation
- STAFS 2007:13 SWEDAC’s Regulations and General Guidelines for Accredited Bodies that Certify Management Systems


B) Safes, bars and locks

Swedish regulations concerning safes, bars and locks include five documents (‘PCC’ stands for Process Certification Clarification and ‘GP’ for General Programme Instruction):

- STAFS 2010:10 SWEDAC’s Regulations and General Guidelines on Accreditation
- PCC Process certification clarification for the international EPD\textsuperscript{382} system
- PCC Process certification for the international EPD system - Guidelines
- STAFS 2013:5 SWEDAC’s Regulations and General Guidelines for Accreditation of Bodies that Certify Products
- IEC GPI General Programme Instruction for Environmental Product Declarations

According to the following figure, numerous normative documents are relevant for safes, bars and locks.

<table>
<thead>
<tr>
<th>Normative document</th>
<th>Product, Product area</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN 14450 Secure storage units - Requirements, classification and methods of test for resistance to burglary</td>
<td>Theft protection cabinets</td>
</tr>
<tr>
<td>EN 215:2004 Thermostatic radiator valves - Requirements and test methods</td>
<td>Radiator thermostat valve</td>
</tr>
<tr>
<td>EN 3-7 Portable fire extinguishers</td>
<td>Portable fire extinguishers</td>
</tr>
<tr>
<td>SS 3492 Secure cabinet - Testing and evaluation of burglary resistance</td>
<td>Safes</td>
</tr>
<tr>
<td>SS 3493 Security cabinet with fire resistance - Specifications for burglary resistance and fire resistance</td>
<td>Safes</td>
</tr>
<tr>
<td>SS-EN 1143-1 Secure storage units - Requirements, classification and methods of test for resistance to burglary - Part 1: Safes, ATM safes, strongroom doors and strongrooms</td>
<td>Safety deposit boxes, ATM-safes, vaults and vault doors</td>
</tr>
<tr>
<td>SS-EN 1143-2 Secure storage units - Requirements, classification and methods of test for resistance to burglary - Part 2: Deposit systems</td>
<td>Deposit safes and service boxes</td>
</tr>
<tr>
<td>SS-EN 1300 Secure storage units - Classification for high security locks according to their resistance to unauthorized opening</td>
<td>High security locks</td>
</tr>
</tbody>
</table>

Source: SWEDAC

Figure 52: Overview of security standards used by DNV Sweden

\textsuperscript{382} Environmental Product Declaration

Page 193 of 542
The figure shows, that several certification services are based on standards, which are only available on a national level. But it should be noted, that while there are several standards available for certification for security (among others, IEC 62642, EN 50131, EN 50133, EN 50136, EN 50518, EN 54 series) none of those listed have been used in the recent years.

DNV also offers certification for quality management systems based on AQAP 2110:2006 NATO quality assurance requirements for design, development and production, AQAP 2120:2006 NATO quality assurance requirements for production and AQAP 2210:2006 NATO quality assurance requirements for software development.

**Svensk Brand- och Säkerhetscertifiering AB (SBSC)**

SBSC is Sweden’s leading organisation for certifying companies, products, management processes and personnel within fire protection and crime prevention. In addition to certificates for individual products and services, SBSC offers system solutions where fire protection and security issues are combined with strategic processes for quality systems and environmental management.

SBSC is owned by the Swedish Fire Protection Association and the Swedish Theft Prevention Association and is accredited by SWEDAC for the certification of products, management processes and individuals, for example based on SS-EN 45011:1998. It is also a member of the European Fire and Security Group (EFSG), which allows approval for products and services in other European countries. SBSC is located in Stockholm and its certification is related with the following logo:

![SBSC Logo](source: SBSC)

**Figure 53: SBSC’s certification mark**

Important certification services offered by SBSC address products and persons: Safes, bars and locks and fire alarm engineers. Safes, bars and locks include:

- Construction hardware - Lock cylinders
- Construction hardware - Locks
- Deposit safes and service boxes
- Emergency fittings
- Grids
- High security locks

---

383 The following sections builds on information from SWEDAC, see http://search.swedac.se/en/accreditations/1631/a001336-001
- Padlock fittings
- Padlocks
- Panic evacuation fittings
- Safes
- Shutters - burglary
- Theft protection cabinets
- Windows and doors - burglary protection
- Wrought-iron gate

Two regulations are relevant in this context:

- STAFS 2010:10 SWEDAC’s Regulations and General Guidelines (STAFS 2010:10) on Accreditation
- STAFS 2013:5 SWEDAC’s Regulations and General Guidelines for Accreditation of Bodies that Certify Products

The certification of persons is based on SS-EN ISO/IEC 17024:2003. The relevant normative document, which defines the characteristics of a competent fire alarm engineer is SBF 1007:4 - Norm for competent engineer fire alarms. The certification scheme builds on two regulations:

- STAFS 2013:6 SWEDAC’s Regulations and General Guidelines for Accreditation of Bodies that Certify Persons and
- STAFS 2010:10 SWEDAC’s Regulations and General Guidelines on Accreditation

According to its website, SBSC also provides certification in the following fields: CCTV installers, CCTV engineers, CCTV system construction (based on several Swedish regulations); persons, products and companies in the field of intruder alarms as well as ‘Certifierad säkerhetschefs’ (persons entrusted with security tasks).384

An interesting aspect is SBSC’s list of gold labeled products. More information is available at http://www.sbsc.se/en/sok/guldmarkta-produkter/

**UL Verification Services**

UL Verification Services offers expertise in commercial testing, inspection and auditing in numerous countries around the world. Of particular interest are UL’s Transaction Security Test Services. UL’s Scandinavian customers use the services of its Danish subsidiary in this regard (UL’s Swedish office does not offer services in the security field).

UL’s transaction security test centers are “certified and accredited to evaluate, execute and manage testing of chip-related products and systems against global regulations, standards and protocols”.385 In cooperation with several certification authorities, processors, acquirers and international brands, UL offers:

---

POS testing, including Common Terminal Acquirer Protocol (C-TAP) and NFC
ATM testing, including bank-specific protocols and functional testing of terminals
Brand testing, including American Express, Diners Club, MasterCard, Visa and others
Card testing, including card personalization evaluations, functional (stress) testing and e-passport (functional) evaluations
Handset testing, including functional testing for schemes such as EMVCo, GFC-PTCRB, Visa and MasterCard
Mobile secure element testing, including functional testing based on the following schemes: EMVCo, GlobalPlatform, Visa, MasterCard, JCB, American Express and Discover
ISO functional testing, including functional testing of contact and contactless cards against ISO 7816 and ISO 10373 standards

UL provides a range of testing services for POS, ATMs, (smart) cards, NFC/TSM, e-identification, and other systems and infrastructures.

Excursus:

UL investigates many additional areas for research purposes, e.g. biometrics for payments and highlights the activities of the Fast IDentity Online (FIDO) Alliance. According to UL, one of the reasons why the financial industry in developed countries is not ready to adopt biometrics is due to the need to comply with strict personal data protection regulations. The need for action is described as follows:

“There is no standard way, to validate the security of biometric data for payments. Security standards and evaluation concepts are needed, which cover the whole chain, including service enrollment, usage, transmission and storage of biometric traits as well as all devices involved in this process. The lack of standardisation can be a barrier to interoperability, especially in an ecosystem where multiple players need to be integrated”.

The FIDO Alliance is regarded by UL as a potential provider of a solution to this problem, which is described as follows:

“FIDO is developing open specifications for strong universal authentication. One of the main goals of this initiative is to supplant the reliance on passwords to securely authenticate users of online services by supporting a full range of technologies, such as fingerprint and iris scanners and voice and facial recognition devices. The major payment schemes have joined the FIDO Alliance along with leading technology companies and banks.”

---

386 Point of Sale
387 Near Field Communication
388 automated teller machine
389 Europay, MasterCard and Visa Contactless Specifications for Payment Systems
390 Global Certification Forum- PCS Type Certification Review Board
LRQA

LRQA is a global certification provider and offers, for example, certificates based on ISO 28000 in the security field. Its Swedish website is http://www.lrqa.se/. LRQA’s assessment process consists of three steps: 1. Visit, 2. Initial Assessment and 3. Surveillance.

LRQA gives the opportunity to transfer existing certification. Organisations, which are already certified based on a management system standard and are thinking about a change, are given the opportunity to make a transition. LRQA offers ‘No-cost, no-obligation quotation’. It will arrange for an assessor to visit with the organisation to initiate a certificate transfer process. The certification transfer process usually involves an examination of the following information:

- Previous visit reports;
- Changes to the organisation and management system;
- Internal and external audit reports;
- Corrective and preventive action;
- Management review;
- Certification, standards and scope; and
- Surveillance programme.

Once this visit has been completed successfully and if there are no issues outstanding, LRQA will issue a new certificate and agree on a surveillance programme. LRQA would normally look to maintain the customer’s current cycle of surveillance and certificate renewal visits.

SIS Förlag AB

Besides standardisation, the Swedish standards body SIS is also active in the certification area. In the security field, SIS is accredited for the certification of persons (“Information Security Management Professional, ISMP”) based on SS-EN ISO/IEC 17024:2003. The activities are based on the aforementioned regulation STAFS 2010:10.

atsec information security AB

Located in Danderyd, the Swedish subsidiary of atsec information security (atsec for short) provides laboratory and consulting services for information security for commercial and governmental sectors. The following aspects summarize its profile:

Relevant accreditation field(s): Laboratory, SS-EN ISO/IEC 17025:2005
Relevant technical field: Safety testing, Information technology
Relevant product/Object: Common Criteria

Three regulations are relevant for atsec’s activities in these fields:

- STAFS 2010:10 The Swedish Board for Accreditation and Conformity Assessment’s (SWEDAC) Regulations and General Guidelines (STAFS 2010:10) on Accreditation
- STAFS 2011:33 SWEDAC’s Regulations and General Guidelines for the Accreditation of Laboratories
- STAFS 2007:20 SWEDAC’s regulations and general guidelines for accreditation of evaluation facilities evaluating IT-security

atsec’s aforementioned characteristics are based on its accreditation by SWEDAC. Together with atsec Germany, atsec AB is accredited in several additional areas by the German certification body DAkkS. atsec’s services related to Common Criteria are also accredited by CSEC (Sveriges Certifieringsorgan för IT-Säkerhet) at the Försvarets Materielverk (FMV). More information on this civil authority under the Swedish Ministry of Defence will be given in the next chapter.

Combitech AB

Combitech is a technical consultancy company for technology, environment and security issues. It has around 20 locations across Sweden, as well as offices in Norway and Finland. Its certification services have many similarities with atsec information security AB and can be summarized as follows:

Relevant accreditation field(s): Laboratory, SS-EN ISO/IEC 17025:2005
Relevant technical field: Safety testing, Information technology
Relevant product/Object: Common Criteria

The regulations are identical with atsec information security AB.

Intertek Certification AB

Intertek Certification is a global company, which tests, inspect and certifies products in 1,000 locations in over 100 countries. Intertek Certification AB is located in Kista. Intertek’s work in the security field is based on two regulations:

- STAFS 2007:13 SWEDAC’s Regulations and General Guidelines for Accredited Bodies that Certify Management Systems
- STAFS 2010:10 SWEDAC’s Regulations and General Guidelines on Accreditation


---

3.8.4.2. PUBLIC SECTOR

This section presents four examples of the public sector. Specific emphasis is put on maritime/port security, aviation security and forensic.

Försvarets Materielverk

Försvarets Materielverk (FMV) is a civil authority under the Swedish Ministry of Defence and has operations in about 80 locations in the country. In the security field, FMV is accredited as an inspection body for SS-EN ISO/IEC 17020:2012.

FMV’s certification services are mainly offered by CSEC. The Stockholm-based office is an independent unit within FMV that was established after a government decision in 2002. CSEC operates as Sweden’s national certification body for IT security in products and systems according to the standard Common Criteria, CC. Certificates issued under the scheme may be subject for mutual recognition according to CCRA, Common Criteria Recognition Arrangement, EA MLA (the EA Multilateral Agreement) as well as SOGIS-MRA, Senior Officials Group Information Systems Security - Mutual Recognition Arrangement.

Like the BSI in Germany for example, CSEC collaborates with accredited external test laboratories. One example is atsec information security AB. As described earlier, atsec is accredited by CSEC to provide Common Criteria-based tests.

Swedish Customs

The Swedish customs is an important player in Sweden’s supply chain security certification, in particular in the area of cargo security. In addition to the security measures adopted by the European Union at the supranational level, Sweden has used the Stairsec programme for several years, which aimed to provide customs compliance and supply chain security. Stairsec was an integrated supply chain security programme developed within Sweden’s Stairway customs accreditation programme, which focused on increasing the quality of customs compliance. The objective of the programme was to increase supply chain security through an accreditation process for all private-sector stakeholders in the international supply chain and terminals. Stairsec became operational with the certification of pilot operators in January, 2004 and mirrored closely the objectives of C-TPAT. Soon after the introduction of the certificate, 40 Swedish companies were certified in Stairsec or in the processing of becoming so. In 2008, the AEO (Authorized Economic Operator) certificate, which represents a common European standard, replaced the Stairsec model.

---

400 atsec, op. cit., no date.
402 Peterson and Treat, op. cit., 2009
**Swedish Maritime Administration**

The Swedish maritime administration offers certification in the fields of maritime security and port security. In response to the events of 11th September, 2001, new rules on maritime security were defined in 2002. They entered into force in July 2004 and comprise extensions of the SOLAS Convention and a new code, called the ISPS Code, which was also attached to the rules in SOLAS. The new rules entered into force in the EU through Regulation (EC) No. 725/2004 on enhancing ship and port facility security. Parallel activities in Sweden included passing an Act (2004:487) on maritime security by Swedish Riksdag, enacted an Ordinance (2004:283) on maritime security by the Swedish Government and issuing a regulation on maritime security, SJÖFS 2004:13, by the Swedish Maritime Administration.

The legislation applies to cargo ships with gross tonnage of 500 or above, passenger ships, mobile offshore drilling units and port facilities that serve such ships engaged in international shipping and passenger traffic between Gotland and the Swedish mainland. After ship security plans are approved and onboard inspections performed, the Maritime Safety Inspectorate issues an International Ship Security Certificate. Likewise, approved and inspected port facilities are given a Statement of Compliance of a Port Facility issued by the Maritime Safety Inspectorate. The foundations for these activities are laid by an additional European document on port security, Directive 2005/65/EC of the European Parliament and of the Council on enhancing port security. The Directive has been transformed into Swedish legislation by law (Act 2006:1209) on port security, the Swedish Government enacted an Ordinance (2006:1213) on port security and the Swedish Maritime Administration issued a regulation on port security, SJÖFS 2007:1.

**Swedish Transportation Agency**

A key player with respect to aviation security in Sweden is the Swedish Transportation Agency. In 2010, it issued for example the Aviation Act (2010:500), which includes several sections regarding security, standards and inspection. According to the Act’s Section 11, the government or public authority appointed by the government may issue regulations to the effect that equipment used in or for aviation shall follow certain standards when the equipment has a bearing on flight safety.

Section 15 highlights the importance of “the Civil Aviation Security Act (2004:1100) and EU legislative instruments for security of aviation at airports etc.” In addition, it outlines that “the government or public authority appointed by the government may, in individual cases, determine that an installation or an activity at an installation used for aviation may not be used or that the activity may not be pursued if the requirements of aviation security are not met, or state under, which conditions the installation may be used or the activity pursued.”

Section 16 adds that “the government or public authority appointed by the government may issue further regulations on access to airports and other aviation installations and on the order there”.

---

403 Amendments to Chapters V and XI-1 and a new Chapter XI-2
Regarding drones, chapter 6 will describe that the European Aviation Safety Agency (EASA) is competent for drones with a Maximal Take-Off Mass (MTOM) above 150 kg that are not used for the military, customs, police, search and rescue, firefighting, coastguard or similar activities or services and are not specifically designed or modified for research, experimental or scientific purposes to be produced in very limited numbers. Authorization of drone operations involving drones with an MTOM of less than 150 kg, in contrast, is to be regulated on a national level.

The authorization of UAV-operations in Sweden is regulated in the Statute Book, the Swedish Transport Agency’s regulations on unmanned aircraft systems (TSFS 2009:88)\textsuperscript{405} published by the Swedish Transport Agency in 2009.

The Swedish Transport Agency is responsible for the authorization of UAV activities that are not regulated by the EASA and respective regulations. In tangible terms, the regulation applies to “design, manufacture, modification, maintenance and operations of civil unmanned aircraft systems below 150 kg MTOM used or designed for: commercial purposes, professional use (not considered as recreation), testing or research, any unmanned flight beyond visual line of sight.”\textsuperscript{406}

The system differentiates between different categories that demand specific provision. The categorization is based on weight, kinetic energy and flight area, e.g. if the UAV is operated within the visual field of the pilot (VLOS) or beyond (BVLOS) and looks as follows:

<table>
<thead>
<tr>
<th>Cat.</th>
<th>Maximal Take-off Mass (MTOM) in kg</th>
<th>Maximal kinetic energy in J</th>
<th>Flight Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>1A</td>
<td>1.5</td>
<td>150</td>
<td>VLOS</td>
</tr>
<tr>
<td>1B</td>
<td>&gt;1.5 - 7</td>
<td>1000</td>
<td>VLOS</td>
</tr>
<tr>
<td>2</td>
<td>&gt;7 - 150</td>
<td>-</td>
<td>VLOS</td>
</tr>
<tr>
<td>3</td>
<td>150</td>
<td>-</td>
<td>BVLOS</td>
</tr>
</tbody>
</table>

Source: Own figure based on material from the Swedish Transport Agency

Figure 54: Categorisation of UAV activities in Sweden

Based on the allocation to a category, specific provisions have to be fulfilled. The provisions are more diverse and strict the higher the category, for example as refered to the skills of the pilots and the amount of information to be provided to the agency. Details concerning the requirements and the authorization process can be withdrawn from chapters 3 to 5 of the Statute Book.\textsuperscript{407} An authorization of a category 3-operation, however, has not been issued to date.\textsuperscript{408}


Stockholm County Police Authority

The Stockholm Country Police Authority is responsible for numerous issues in the security field. This section highlights its specific activities in the field of forensic.

Within the EU, forensic analysis of fingerprints must be accredited not later than 30th November 2015. In Sweden, the Technical Division at the Stockholm County Police Authority was the first to adapt to the requirement. In 2008, the EU countries adopted a Council Decision – the so-called Prüm Decision – concerning intensified cross-border collaboration to fight terrorism and crime through automated exchange of DNA profiles, fingerprints and information from vehicle registers.

During the Swedish Presidency of the EU in 2009, an agreement was reached within the EU Council for Legal and Domestic Issues to introduce accreditation as a requirement for the analysis of DNA and fingerprints, in order to safeguard quality. The requirement applies as from 30th November 2013 for DNA, and from 30th November 2015 for fingerprints.

In Sweden, the Stockholm County Police Authority was appointed the 'pilot authority', and in 2010 the work of accreditation begun at the laboratory at the Technical Department. Around 15 methods are used by the laboratory in the analysis work, of which ten have been accredited to SS-EN ISO/IEC 17025 so far. In the preparation work ahead of the accreditation, the department has collaborated with national and European laboratories with well-developed systems for quality assurance of forensic work.

The department is currently defining the procedures that will apply during crime scene investigations in order to protect and look after traces. It is also represented in the Swedish committee taking part in the work of developing standards for handling forensic material, at crime scenes and elsewhere. In fact, needs for new standards remain: “The standard that can currently be used for crime scene investigations is the more general ISO 17020. With a sector-specific standard, the requirements would be clearer”, explained another expert. The laboratory at the Stockholm Police received its accreditation at the end of May 2013. 409

FOI

FOI is one of Europe’s leading research institutes in the areas of defence and security. Its core activities are research, methodology/technology development, analyses and studies. FOI is an assignment-based authority under the Ministry of Defence. FOI has “one of the few security classified CBRN laboratories in Europe that is licensed to receive and examine all types of hazardous substances.” 410 FOI’s security laboratory is accredited by SWEDAC. 411

3.8.5. **SUMMARY AND CONCLUSION**

Sweden has a committed security industry and is an active player in international security standardisation. Its StairSec program played a pivotal role in the development of the harmonized European AEO program which is regarded as good practice. Standards developed for European ABC systems and CBRN protection, as well as the LRQA approach to handling external certification and solutions in the biometric field, are also unique in nature and considered good practice. Sweden has also one of the few security classified CBRN laboratories in Europe, FOI, that is licensed to receive and examine all types of hazardous substances, indicating strong and well-structured security infrastructure. Furthermore, as of November 30, 2015, Sweden requires the accreditation of public authorities. Challenges related to the mutual recognition of certification are nonetheless present with the certification of safes based on the national standards SS 3492 and SS 3493 serving as an example.

3.8.6. **REFERENCES**

atsec, Common Criteria Zertificate, no date.


LRQA, “Certifiering och verifiering av ledningssystem”, no date.
http://www.lrqa.com/services-we-offer/certification/assessment-process


SP, “Control units for cash registers”, no date.
http://www.sp.se/en/index/services/certprod/certprodprofil/elektronik/kassaregk/Sidor/default.aspx


SWEDAC, SWEDAC’s Database on accredited bodies, Forensic analysis, no date. http://search.swedac.se/en/accreditations?mode3_accarea_l1=Forensic+analysis&mode3_acccarea_l2=&mode3_accastd=&mode3_docs=


3.9. **United Kingdom**

3.9.1. **Introduction**

This section contains a case study of the UK Security Industry, specifically with regard to standardisation and certification of security PSS. The report provides an identification and overview of key certification bodies, their standards and schemes. Through desk research and interviews with key stakeholders in the above fields, best practice standards and certification schemes were identified and these are presented in the following sections.

3.9.2. **Short Description of the UK Security Industry**

The UK Security sector’s definition was first agreed in 2007/08. As a constantly changing sector, the definition was updated in 2011 to include cyber security activities and again in 2013 to reflect changes in content and reporting of cyber activities.

According to a KMatrix estimate, the UK share of the global security market is worth more than 4 %, (£3.2Bn), which places the UK as the sixth largest exporter of new security products and services. Around 40% of UK exports can be attributed to Cyber Security products and services. The UK domestic market for security products is valued at £1.8 bn annually. The UK Trade & Investment Defence & Security Organisation (UKTI DSO) makes note that the numbers compiled by KMatrix do not in all instances capture UK Private Security company data, so these figures are estimates, however built on rigorous research.

Cyber security has also been emphasised as an emerging sector in the National Security Technology Procurement (mentioned below) and the commitment of the UK government to “work with industry to establish robust cyber security standards which ensure that our key contractors in areas of national security importance (such as defence) act to protect sensitive information and systems against cyber-attack.” This situation is reflected as a current market trend in the Global Safety and Security Resource Guide of the U.S. Department of Commerce, International Trade Administration.

---


The UK Government’s white paper *National Security Through Technology*\(^\text{418}\) recognises the UK security and defence industries as dynamic and successful to export, as, in addition to raising revenue, it allows for the building of bilateral relationships and cooperation with key allies more so than any other industry. Exporting and relationship building is also seen to help tackle threats to UK national security.

<table>
<thead>
<tr>
<th>UK Security Sub-Sectors</th>
<th>General</th>
<th>Cyber Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Access Control Systems</td>
<td>• Forensics &amp; Evidence</td>
<td>• Cyber Consultancy</td>
</tr>
<tr>
<td>• Ancillary Security Equipment &amp;</td>
<td>• Information &amp; Data Security</td>
<td>• Encryption</td>
</tr>
<tr>
<td>• Services</td>
<td>• Intruder Alarm Systems</td>
<td>• Identify &amp; Access- Based Services</td>
</tr>
<tr>
<td>• Audio Equipment &amp; Systems</td>
<td>• Manned Security Systems</td>
<td>• Infrastructure</td>
</tr>
<tr>
<td>• Biometrics</td>
<td>• Personal Protection &amp; Control</td>
<td>• Mobile Security</td>
</tr>
<tr>
<td>• Bomb Disposal, Explosives &amp;</td>
<td>• Security Hardware</td>
<td>• Outsourced/ Managed Services*</td>
</tr>
<tr>
<td>• Ballistics</td>
<td>• Sensing Systems &amp; Heads</td>
<td>* 2013 additions are shown in blue</td>
</tr>
<tr>
<td>• CBRN &amp; Anti Terrorism</td>
<td>• Tracking Systems</td>
<td></td>
</tr>
<tr>
<td>• CCTV &amp; Associated Systems</td>
<td>• Vehicles</td>
<td></td>
</tr>
<tr>
<td>• Communications</td>
<td>• Weapons &amp; Ammunition</td>
<td></td>
</tr>
<tr>
<td>• Fire, Noxious Fumes &amp; Flooding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarms</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: KMatrix, 2014\(^\text{419}\)

Figure 55: UK security sub sectors

The white paper also stipulates that in order for the security and defence export sectors to grow at a faster rate, it is imperative that all PSS be high quality and developed according to the highest standard. The white paper furthermore reveals the government’s evaluation of potential benefits of appointing a Senior Responsible Owner (SRO) within Government to head up a security authority and the merits of developing a UK Security Brand. This indicates governmental support to strengthen the UK security industry.

### 3.9.2.1. SELECTED POLICY, REGULATION AND LEGISLATION

For the purpose of this report, thought was given to the remit of the concept of security and whether a line should be drawn to separate private security from national security or state se-

---

\(^{418}\) Ministry of Defence, op. cit., 2012.

\(^{419}\) Ministry of Defence, op. cit., 2012. p. 4
It is clear that a great majority of PSS are used across the two fields and as Button (2008, p. 5 – cited in Gill, et al., 2012, p. 16) has argued: “Internationally there is no security function carried out in the state sector that is not undertaken in the private sector in some form.” We thus decided in this report to refer to security technologies, systems and services without explicitly demarcating their field of operation. However, we have attempted to exclude from analysis standards and certification relevant to Health & Safety and Defence – although the lines may at times seem blurred between these fields. This section outlines the key regulatory, legislative and policy documents which are relevant to the remit of this report. They were selected on the basis of references in interviews and in documents regarding standards and certification of security PSS.421

The Private Security Industry Act 2001

The Private Security Industry Act of 2001 is the legal framework which regulates the UK private security industry. Before 2001 there had been little, no or self-regulation and standards across the industry varied widely. The key aim of the Act was to raise standards across the board and protect and reassure the public by preventing unsuitable people getting into positions of trust. Under the 2001 Act the following security practices required licencing:

- Door Supervisors
- Vehicle Immobilisers (Wheel Clampers)
- Manned Guarding
- Keyholders
- Security Consultants
- Private Investigators

The Private Security Industry Act furthermore mandated the foundation of the Security Industry Authority (SIA), which now covers the licencing of the above services and in 2015 will extend licensing into producing licences for businesses in addition to individuals as it has done until now. Further elaboration on the role of the SIA is provided in section 3.9.7.

UK Cyber Security Strategy 2011

UK Security policy and industry reports acknowledge the emergent security questions which emerge in Cyberspace and the UK Cyber Security Strategy, published in 2011 which sets the vision for 2015 “to derive huge economic and social value from a vibrant, resilient and secure


Page 207 of 542
cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society”. To this end, the strategy sets out four key objectives:

1. To tackle cyber-crime and be one of the most secure places in the world to do business in cyberspace
2. To be more resilient to cyber-attacks and better able to protect its interests in cyberspace
3. The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies
4. The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all its cyber security objectives

The strategy outlines a number of measures that the UK Government aims to take in order to achieve the above objectives of which the most relevant for this report is the focus on standards and how the Department for Business, Innovation and Skills will work with “domestic, European and global and commercial standards organisations to stimulate the development of industry-led standards and guidance that help customers to navigate the market and differentiate companies with appropriate levels of protection and good cyber security products.”

**CCTV Code of Practice**

The CCTV Code of Practice from 2014 “provides good practice advice for those involved in operating CCTV and other surveillance camera devices that view or record individuals, and covers other information that relates to individuals, for example vehicle registration marks captured by Automated Number Plate Recognition (ANPR) equipment.” This most recent version is an update of the original code of practice, published in 2000. The importance of this document is stressed by the British Security Industry Association (BSIA), the Security Industry Authority (SIA) and by several certification bodies that deal with certification of CCTV and surveillance cameras. Users and operators of CCTV cameras are urged to comply with the code in addition to established standards. The code recognises the proliferation of CCTV in UK society where surveillance cameras are operated by a wide range of individuals within public and private sphere for various purposes. The regulatory environment and the code of practice are seen as a step towards simplifying and streamlining CCTV regulation for users and operators. The code also provides information to citizens regarding their rights as they are increasingly under surveillance in daily life.

With regard to standards, the code refers to the Protection of Freedoms Act (POFA), which should work in conjunction with the CCTV code of practice, and “provides guidelines on operational requirements, technical standards and effectiveness of systems available.” One of the POFA guiding principles states that:

---


425 Information Commissioners Office, op. cit., 15.10.2014.
“Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.”

POFA also outlines guidance on privacy with regard to data collection and storage, and possible impact on individuals. It also stresses the importance of clear accountability and responsibility with regard to operation of surveillance cameras.

The CCTV Code of practice provides CCTV operators and users with a checklist which assists with making sure that all necessary actions have been taken, and that the review of these is planned with regular intervals.

### 3.9.2.2. The British Security Industry Association (BSIA)

The BSIA is a trade association which covers all aspects of the professional security industry in the UK and represents almost 600 member companies from across 15 different security sectors.\(^{427}\) The BSIA and its members participate in British and European Standards development and revisions to ensure that the industry is kept up to date with the latest changes in the landscape. Furthermore, the association lobbies and influences legislative changes to the private security industry in the UK. The BSIA estimate that their member companies provide over 70% of UK security products and services.

In order to pass for membership at the BSIA companies must pass strict entry criteria, one of which is compliance to industry standards. Firstly, “all members are required to achieve and maintain accreditation to ISO 9001:2000 and be inspected to relevant British Standards through a UKAS accredited certification body.”\(^{428}\) The figure below lists selected key standards presented by the BSIA on their website:

<table>
<thead>
<tr>
<th>Sector</th>
<th>Relevant Standards, codes of practice and regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control</td>
<td>BS EN 50133-1:1997 System requirements for access control systems</td>
</tr>
<tr>
<td></td>
<td>BS EN 50133-2:2000 Component requirements for access control systems</td>
</tr>
<tr>
<td></td>
<td>BS EN 50133-7:1999 Application guidelines for access control systems</td>
</tr>
<tr>
<td></td>
<td>SSAIB Code of Practice for Access Control Systems (SSAIB(^{429}))</td>
</tr>
<tr>
<td></td>
<td>PAS(^{430}) 68: 2010 Impact test specifications for vehicle security barriers (BSI)</td>
</tr>
<tr>
<td></td>
<td>NCP 109 NSI Code of Practice for Planning, Installation and Maintenance of Access Control Systems (NSI)(^{431})</td>
</tr>
</tbody>
</table>

---

\(^{426}\) Information Commissioners Office, op. cit., 15.10.2014 p. 43

\(^{427}\) British Security Industry Association, “Why use a BSIA guarding company?”, no date.

http://www.bsia.co.uk/web_images/publications/guarding_benefits_april08.pdf

\(^{428}\) British Security Industry Association, op. cit., no date.

\(^{429}\) SSAIB provides certification for security service providers

\(^{430}\) Public Available Specification (PAS) is a fast track standard which is market driven but produced by the BSI. After two years a PAS can go forward to become a formal British Standards.

\(^{431}\) National Security Inspectorate provides certification for security service providers

### PAS 68: 2010 Impact test specifications for vehicle security barriers (BSI)

### TS201: Enhanced security requirements for doorsets and door assemblies for dwellings to satisfy the requirements of PAS23 and PAS24, (Warrington Certification)

### STS202: Requirements for burglary resistance of construction products including hinged, pivoted, folding or sliding doorsets, windows, curtain walling, security grilles, garage doors and shutters (Warrington Certification)

### IEE Wiring Regulations

### LPS 1175 Requirements and testing procedures for the LPCB approval and listing of intruder resistant building components, strongpoints, security enclosures and free standing barriers (LPCB)

### Asset and property marking

| BS 7858: 2006 + A2: 2009 Security screening of individuals employed in a security environment – Code of Practice |
| LPS 1224: Issue 2 or later Requirements for companies providing secure asset registration services |
| LPS 1225: Issue 3 or later Requirements for the LPCB Approval and Listing of Asset Marking Systems |
| PAS 40: 2002 Banknote theft deterrent systems using dye or smoke-dye |
| BSIA Code of Practice – Manufacture, application & Data recording of asset marking systems |

### CCTV

| BS EN 62676 series Video surveillance systems for use in security applications |
| BS EN 62676-1-1 Video System Requirements |
| BS EN 62676-1-2 Video Transmission – General Video Transmission – Requirements |
| BS EN 62676-2-1 Video Transmission Protocols – General Requirements |
| BS EN 62676-2-2 Video Transmission Protocols – IP Interoperability implementation based on HTTP and REST services |
| BS EN 62676-2-3 Video Transmission Protocols – IP Interoperability implementation based on web services |
| BS EN 62676-3 Analog and Digital Video Interfaces |

---

432 Loss Prevention Certification Board (LPCB)
<table>
<thead>
<tr>
<th>Standard/Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BS EN 62676-4</td>
<td>Application guidelines</td>
</tr>
<tr>
<td>BS EN 60529</td>
<td>Degrees of Protection provided by Enclosures (IP Code)</td>
</tr>
<tr>
<td>BS EN 62305</td>
<td>series Protection against Lightning</td>
</tr>
<tr>
<td>BS EN 50132-7</td>
<td>CCTV surveillance systems for use in security applications: Application guidelines</td>
</tr>
<tr>
<td>BS EN ISO 11064-1</td>
<td>Ergonomic design of control centres Principles for the design of control centres</td>
</tr>
<tr>
<td>BS EN ISO 11064-2</td>
<td>Ergonomic design of control centres Principles for the arrangement of control suites</td>
</tr>
<tr>
<td>BS EN ISO 11064-3</td>
<td>Ergonomic design of control centres Control room layout</td>
</tr>
<tr>
<td>BS 5979</td>
<td>Remote centres receiving signals from fire and security systems. Code of practice</td>
</tr>
<tr>
<td>BS 7671</td>
<td>Requirements for electrical installations. IET Wiring Regulations.</td>
</tr>
<tr>
<td>BS 7958</td>
<td>CCTV Management and Operation – Code of Practice</td>
</tr>
<tr>
<td>BS 8418</td>
<td>Installation and remote monitoring of detector activated CCTV systems – Code of practice</td>
</tr>
<tr>
<td>BS 8495</td>
<td>Code of Practice for digital CCTV recording systems for the purpose of image export to be used as evidence</td>
</tr>
<tr>
<td>BS 8591</td>
<td>Remote centres receiving signals from alarm systems – code of practice</td>
</tr>
<tr>
<td>BS 10008</td>
<td>Evidential weight and legal admissibility of electronic information. Specification</td>
</tr>
<tr>
<td>PSDB 09/05</td>
<td>HOSDB/ACPO UK Police Requirements for Digital CCTV Systems</td>
</tr>
<tr>
<td>BSIA Form 120</td>
<td>Code of practice for the maintenance of CCTV systems</td>
</tr>
<tr>
<td>BSIA Form 197</td>
<td>CCTV Privacy Masking Guide</td>
</tr>
<tr>
<td>BSIA Form 199</td>
<td>CCTV Chip and PIN Guide</td>
</tr>
<tr>
<td>BIP 0008-1</td>
<td>Code of Practice for Legal Admissibility and evidential weight of information stored electronically</td>
</tr>
<tr>
<td></td>
<td>BS 7858 Security screening of individuals employed in a security environment. Code of practice</td>
</tr>
</tbody>
</table>
| **Lone workers** | BS 8484: 2009 Code of practice for the provision of lone worker device (LWD) services  
BS EN 50518-3:2013 Monitoring and alarm receiving centre. Procedures and requirements for operation |
| **Property and asset protection** | BS 7858 Security screening of individuals employed in a security environment - Code of Practice  
BS 7984:2008 Key-holding and response services. Code of practice  
PD 6662 Scheme for the application of European standards for intrusion and hold-up alarm systems  
EN 50131-1 Alarm systems. Intrusion and hold-up systems – System requirements  
TS 50131-7 Alarm systems. Intrusion and hold-up systems – Application guidelines  
BS 8243 Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions. Code of practice  
DD 263 Intruder and hold-up alarm systems. Commissioning, maintenance and remote support. Code of practice  
BS 8484 Provision of lone worker device (LWD) services – Code of practice  
BS 5979 Remote centres receiving signals from fire and security systems. Code of practice  
BS 8591 Remote centres receiving signals from alarm systems. Code of practice  
BS EN 50518 Monitoring and Alarm Receiving Centres  
BSIA also recommend that doors and locks produced to specific BS standards be procured to enhance property and asset protection. |
| **Security equipment manufacturers** | For manufacturers of Alarm Systems BSIA refer to the following standards:  
EN 50136 family of standards for Alarm Systems, Alarm transmission systems and equipment  
BS EN 50131 standards that specify general requirements for Intruder and Hold-up Alarm Systems  
PD 6662:2010 Scheme for the application for European standards for intruder and hold-up alarm systems  
DD CLC/TS 50131-3 Intruder Alarms, Control and Indicating Equipment Requirements |
Security guarding

BS7499: 2007 Code of practice for static site guarding and mobile patrol services
BS7984: 2001 Code of practice for keyholding and response services
BS7858: 2006 Code of practice for security screening of personnel employed in a security environment

Source: BSIA
Figure 56: Key standards for the British security industry

3.9.3. THE SECURITY STANDARDISATION FRAMEWORK

The Security standardisation frameworks consists of the British Standards Institution (BSI) which is the National Standards Body for the UK, United Kingdom Accreditation Service (UKAS) which is the national accreditation body and a great number of conformity assessment and certification bodies which certify and assess conformity against International standards, European Standards and British Standards. This section will examine and present detailed information about each of the above institutions. A selection of certification bodies will be examined in detail in chapter 3.9.5.

Source: The Chartered Quality Institute
Figure 57: The UK quality infrastructure

The above diagram, although of the UK Quality landscape, gives a good overview of the relationship and key organisations within the UK standardisation framework. “Bodies shown in

---

433 The Chartered Quality Institute, op. cit., 2014
black are sponsored by Government and receive some funding for their activities. Bodies shown in blue are self-funded and independent of Government. (Note: The British Standards Institution is an exception, in that the BSI Group comprises the UK’s National Standards Body - BSI British Standards, which does receive funding, also a certification body - BSI Management Systems and a testing operation - BSI Product Services).”

3.9.3.1. **BRITISH STANDARDS AGENCY (BSI)**

The Department for Business, Innovation and Skills (BIS) is responsible for UK government policy on standards development and as such sponsors and works closely with the British Standards Institution (BSI) which is the UK National Standards Body. The BSI was the first national standards body when it was established in 1901. BSI has 72,000 clients operating in 150 countries and published 2,500 standards in 2014.435

A memorandum of understanding between the UK Government and BSI states that they agree that the definition of an NSB should be “interpreted to include the management, coordination and undertaking of:

(i) “British Standards” and “other standardisation products”;
(ii) participation by BSI in European and international standards bodies, and other international activity undertaken in the interests of BSI as the United Kingdom’s NSB;
(iii) promotion, marketing, distribution and information activities concerned with British Standards, BSI’s other standardisation products, and standardisation generally;
(iv) support and corporate infrastructure activities intended, wholly or in part, to enable (i)-(iii) above”436

With regard to standards development, there are currently 1,350 BSI committees with around 10,000 voluntary members that work on developing standards. BSI offers training in standardisation processes, issues and bodies and committees are supported by BSI staff. BSI requires all committees represent the interests of users, manufacturers, government and any other groups or organisations relevant to their work.

In addition to standards which are developed by public consultation and consensus, the other types of standards BSI develops are:

- **PAS (Public Available Specifications)**, which are fast track and temporary standards, which can become a British Standard after two years if its foundation and specification is clear and robust. PAS are sponsored by an interested party (e.g., company or organisation) when they quickly need a standard for a specific market need.
- **PD (Published Documents)** include “standards-type documents that don’t have the same status as British Standards and come under the catch-all category of Published


Documents (PD). These are provisional and often subject to further developments on the basis of experience.

Further to standardisation, BSI is also the owner and operator of BSI Kitemark™, which is a registered and well recognised certification mark in the UK and internationally. The Kitemark scheme is accredited by UKAS and offers risk reduction, increased customer satisfaction and access to new markets. The Kitemark™ scheme will be discussed in more detail in chapter 3.9.5.

One of the sectors BSI develops and provides standards for is Security. The aim of standards within the security sector is to adopt a practical approach to security in order to “minimize risks, avoid litigation, reduce insurance premiums and meet regulatory requirements”.

BSI works on Security Standards development within the following fields. The figure demonstrates which standards are currently in use, be they British, European or International:

<table>
<thead>
<tr>
<th>Field</th>
<th>Standards Development – Established Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometrics</td>
<td>BS ISO/IEC Standards</td>
</tr>
<tr>
<td>Data protection</td>
<td>BS Standard</td>
</tr>
<tr>
<td>Electronic security systems</td>
<td><strong>Intruder alarm systems</strong></td>
</tr>
<tr>
<td></td>
<td>BS and BS EN Standards</td>
</tr>
<tr>
<td></td>
<td><strong>CCTV</strong></td>
</tr>
<tr>
<td></td>
<td>BS and BS EN Standards</td>
</tr>
<tr>
<td></td>
<td><strong>Identification card systems</strong></td>
</tr>
<tr>
<td></td>
<td>BS ISO and BS EN Standards</td>
</tr>
<tr>
<td></td>
<td><strong>Retail banking</strong></td>
</tr>
<tr>
<td></td>
<td>BS ISO Standards</td>
</tr>
<tr>
<td>Fire protection equipment</td>
<td><strong>Fire detection and alarm systems</strong></td>
</tr>
<tr>
<td></td>
<td>BS Standards</td>
</tr>
<tr>
<td></td>
<td><strong>Fire sprinkler systems</strong></td>
</tr>
<tr>
<td></td>
<td>BS, BS EN, BS ISO and ISO Standards</td>
</tr>
<tr>
<td>Information security</td>
<td>BS and BS ISO/IEC Standards</td>
</tr>
<tr>
<td>IT network security</td>
<td>BS ISO/IEC Standards</td>
</tr>
<tr>
<td>People &amp; Employee security</td>
<td>BS and BS EN standards</td>
</tr>
<tr>
<td>Physical security</td>
<td>BS Standards</td>
</tr>
<tr>
<td>Vehicle security</td>
<td>BS EN Standards</td>
</tr>
</tbody>
</table>

Source: Own figure
Figure 58: Origin of currently used security standards in the UK

In addition to standards development, BSI offers security-related training courses e.g., Implementing ISO/IEC 27001Information Security, BCS Certificate in Data Protection and BCS Practitioner Certificate in Information Risk Management.

---

3.9.3.2. THE UK ACCREDITATION SERVICE (UKAS)

United Kingdom Accreditation Service (UKAS) is a non-profit private company and is recognised by the UK Government as the national accreditation body for the UK. Its remit is to “assess, against internationally agreed standards, organisations that provide certification, testing, inspection and calibration services.” UKAS is licensed by The Department for Business, Innovation and Skills to “use and confer the national accreditation symbols which symbolise Government recognition of the accreditation process.”

Accreditation by UKAS, as a third party, is recognition of competence to perform specific tasks, be it a test laboratory, certification body or an inspection body and means they have been evaluated and assessed against internationally recognised standards. UKAS is a member of European Accreditation.

A search for accredited certification bodies which deal with Security returns 83 separate listings. In chapter 3.9.5 some of these certification bodies and their schemes will be examined and analysed in further detail.

3.9.3.3. UK ISO TC PARTICIPATION

<table>
<thead>
<tr>
<th>ISO TC</th>
<th>Topic</th>
<th>Participation (P-/O-Member)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC/JTC 1/SC 17</td>
<td>Cards and personal identification</td>
<td>P, secretary</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 27</td>
<td>IT Security techniques</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 31</td>
<td>Automatic identification and data capture techniques</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 37</td>
<td>Biometrics</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 68</td>
<td>Financial services</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 85</td>
<td>Nuclear energy, nuclear technologies, and radiological protection</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 92</td>
<td>Fire safety</td>
<td>P, secretary</td>
</tr>
<tr>
<td>ISO/TC 223</td>
<td>Societal security</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 224</td>
<td>Service activities relating to drinking water supply systems and wastewater systems - Quality criteria of the service and performance indicators</td>
<td>P</td>
</tr>
</tbody>
</table>

439 UKAS is appointed as the UK National Accreditation Body by The Accreditation Regulations 2009 (SI No 3155/2009) and operates under an MoU with the Secretary of State for Business, Innovation and Skills.


441 United Kingdom Accreditation Service, op. cit., no date.
3.9.4. Selected EN and ISO Standards and their application in the UK

The figure below features selected standards and an overview of to what extent these standards are used in the UK for certification purposes.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Accredited CBs which offer certification services based on the standard</th>
<th>Names of the certification bodies</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN ISO 27799</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>EN 13094</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>EN 14025</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>EN 12972</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>ISO 28000</td>
<td>3</td>
<td>MSS Global Ltd</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lloyds Register Quality Assurance Ltd.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reynolds Technological Inquiries Ltd.</td>
</tr>
<tr>
<td>EN ISO 22301</td>
<td>8</td>
<td>Examples:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DNV Certification Ltd.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ascertiva Group Limited Trading as NQA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BSI Assurance UK Ltd</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intertek Certification Ltd</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lloyds Register Quality Assurance Ltd</td>
</tr>
<tr>
<td>EN 14339</td>
<td>2</td>
<td>SGS United Kingdom Ltd</td>
</tr>
<tr>
<td>EN 14384</td>
<td>2</td>
<td>BSI Assurance UK Ltd</td>
</tr>
</tbody>
</table>

Figure 60: British certification bodies in selected fields

3.9.5. The Security Conformity Assessment Framework

In the UK Department for Business, Industry and Skills (BIS) is responsible, on behalf of the Government, for the horizontal policy on standards, accreditation and conformity assessment. In short, conformity assessment is the process and verification that what is supplied (product, system or service) meets the standards or requirement claimed.

“Conformity assessment bodies fall into two categories (ISO/IEC 17000):

- those concerned with assessment, e.g. testing laboratories or inspection bodies
those concerned with third-party attestation (i.e. assurance that specified requirements are fulfilled) of product conformity, management systems conformity or fulfillment of requirements for personal competence - known collectively as certification bodies.

The figure below presents a selection of UK Inspection bodies and testing labs accredited by UKAS. Selection was made by presenting here as great variety as possible of testing labs, rather than presenting all 61 testing labs that resulted from a search in the UKAS database using the search term ‘security’. Certification bodies are presented in detail in chapter 3.9.5.

<table>
<thead>
<tr>
<th>Company name</th>
<th>Category</th>
<th>Key security activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groundwork Wales</td>
<td>Inspection body</td>
<td>Social security inspection</td>
</tr>
<tr>
<td>Ascertiva Group Ltd</td>
<td>Inspection body</td>
<td>Social security inspection</td>
</tr>
<tr>
<td>CCQS UK Ltd</td>
<td>Inspection body</td>
<td>Physical security of equipment</td>
</tr>
<tr>
<td>AJA Registrars Ltd</td>
<td>Inspection body</td>
<td>Social security inspection</td>
</tr>
<tr>
<td>NCC Group</td>
<td>Testing lab</td>
<td>Information and IT security</td>
</tr>
<tr>
<td>Context Information Security Ltd</td>
<td>Testing lab</td>
<td>Information and IT security</td>
</tr>
<tr>
<td>Build Check Ltd</td>
<td>Testing lab</td>
<td>Product and building testing (windows, glass, doors)</td>
</tr>
<tr>
<td>SiVenture</td>
<td>Testing lab</td>
<td>Information and IT security (hardware testing)</td>
</tr>
<tr>
<td>Wintech Engineering Ltd</td>
<td>Testing lab</td>
<td>Product and building testing (windows, glass, doors)</td>
</tr>
<tr>
<td>BRE Global Ltd</td>
<td>Testing lab, certification, inspection</td>
<td>Product and building testing. Fire systems, alarm systems, windows, doors, locks</td>
</tr>
<tr>
<td>BSI Assurance Ltd</td>
<td>Testing lab, certification body, standardization body</td>
<td>Product testing. Locks, doors, windows, fire detection and alarm systems, protective clothing</td>
</tr>
<tr>
<td>3M Security Systems Division</td>
<td>Testing lab</td>
<td>Machine readable travel documents</td>
</tr>
<tr>
<td>Assa Abloy Test Laboratory</td>
<td>Testing lab</td>
<td>Locks</td>
</tr>
</tbody>
</table>

Figure 61: Overview of British certification bodies and their services in the security field

Lewis (2014) presents additional services. Certification for CCTV and video technology as well as access control systems is offered by the Security systems and Alarms Inspection Board (SSAIB). The certification scheme will be investigated in detail in CRISP’s work package 4. According to the source, the UK Home Office Centre for Applied Science and Technology (CAST) has also developed a standard called i-LIDS for the advanced capabilities of advanced CCTV systems, which carry out intelligent processing on CCTV to infer use-

---

ful security information, referred to as video analytics. It also offered certification to it.\textsuperscript{444} The certification task is now entrusted to BRE and its Video Analytics Assessment Programme. More information is given at \url{http://www.bre.co.uk/page.jsp?id=2770} as well as in the next chapter.

Another interesting solution is offered in the biometrics field: the UK National Physical Laboratory NPL undertakes testing of the biometric component of physical access control systems to secure an area within a building against a UK government standard.\textsuperscript{445}

The BSI also operates a Security Industry Authority-Approved Contractor Scheme (SIA-ACS).\textsuperscript{446} More information on this scheme is given in the next chapter.

\section*{3.9.6. \textit{Selected Security Certification Bodies and Their Work}}

The UKAS Search Engine delivers 83 results for the search term ‘security’ listing relevant certification bodies. For the purpose of this report we explore in depth 4 certification bodies, which were selected on the basis of desk research and interviews undertaken in the project, and on the basis of rank on the UKAS website. A full list of certification bodies in the UK that certify security PSS is available on the UKAS website.

\subsection*{BSI Assurance}

In addition to developing standards, BSI offers testing and certification services including pre-assessment, gap analysis, batch testing and full compliance testing. BSI, is furthermore a Notified Body for CE marking and owner of the well-recognised flagship scheme Kitemark\textsuperscript{\textregistered} The Kitemark\textsuperscript{\textregistered} scheme is accredited by UKAS and is a conformity certification trademark and was originally used only in the UK but is now recognised internationally. The Kitemark\textsuperscript{\textregistered} schemes are available for a variety of products and services that fall within the following sectors:

- Automotive
- Construction
- Electrical
- Emergency lighting and luminaires
- Energy
- Financial products
- Fire
- Flood protection
- IT and digital transactions
- Personal Protective Equipment
- Removal Services.

\textsuperscript{444} Lewis, op. cit., 2014, p. 15
\textsuperscript{445} Lewis, op. cit., 2014, p. 15
\textsuperscript{446} Lewis, op. cit., 2014, p. 21
With regard to Security, it is not presented as a separate scheme; however security related products and services do fall under the above sectors. In order to present an example two categories deemed most relevant to the CRISP project were researched further.

**IT and Digital Transactions**

To achieve the Secure Digital Transactions Kitemark™ websites and apps are rigorously and independently tested for financial and personal information security. The tests are both internal and external penetration tests, which scan for vulnerabilities and security flaws. The seal is awarded to websites or apps that facilitate different kinds of online transactions.

![BSI Secure Digital Transactions Kitemark™](image)

Source: BSI

Figure 62: BSI secure digital transactions KITEMARK™

This scheme is voluntary and only available from the BSI. After certification the process is ongoing to ensure high levels of security. If already Kitemark™ websites or apps fail testing, the Kitemark™ can be taken away. The assessment involves testing and assessment according to ISO 27001 for any section of a business that handles confidential data. The Kitemark™ is awarded against the website or app but not to the provider itself.

**Personal Protective Equipment**

BSI certification extends to a broad range of protective clothing, including:

- Impact protection
- Respiratory, hearing and eye protection
- Protective clothing (flame retardant, high visibility and CBRN protection)

All BSI testing is carried out against combined risks, flame retardant and high visibility. All standards listed in this certification category are European (BS EN) or international (BS ISO) standards. Selected featured standards in this category are shown in Figure 63.

<table>
<thead>
<tr>
<th>Standard Reference Number</th>
<th>Standard Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>BS EN 464:1994</td>
<td>Protection against liquid and gaseous chemicals, including aerosols and solid particles</td>
</tr>
<tr>
<td>BS EN 14116:2008</td>
<td>Protective clothing against heat and flame</td>
</tr>
<tr>
<td>BS EN ISO 17491-4:2008</td>
<td>Protection against liquid chemicals</td>
</tr>
</tbody>
</table>

Figure 63: Relevant standards for BSI’s certification services in the security field
BRE/ BRE Global Ltd

BRE (Building Research Establishment) has an extensive experience and long history, dating back 90 years. As the name indicates (the organisation was previously named the Building Research Station) BRE’s work centres on the built environment, and extends to the testing and certification of security products, such as alarm systems, fire safety, personal protection etc. BRE is known internationally and carries out its certification work through BRE Global Ltd, which is an independent third party certification body offering certification of fire and security products/services to an international market.

BRE Global Ltd offers certification schemes within the following CRISP relevant fields:

- Automatic sprinkler systems
- Firebreak doors and shutters
- Fire detection and alarms
- Fire resistant cables
- Fixed firefighting systems
- Installers
- Manual extinguishing equipment
- Passive fire protection
- Quality management systems
- Smoke & ventilation systems
- Security protection products.

One of the scheme that BRE certifies security and fire systems under is the Loss Prevention Certification Board (LPCB), which is a well known scheme with a well recognised mark.

Source: LPCB
Figure 64: LPCB certification mark

The Loss Prevention Certification Board (LPCB) has been working with industry and government for more than 100 years to set the standards needed to ensure that fire and security products and services perform effectively. LPCB, which works with industry and government in the development of standards, offers third-party approval confirming that products and services have met and will continue to meet these standards. LPCB laboratories are independently accredited by UKAS.

The Loss Prevention Standards (LPS) are produced when a new unproven technology is introduced, to help ensure that the product/service meets the needs of users, they also help address risks that are not covered by covered by existing national and international standards.
and codes. The standards are developed by teams of experts, and are reviewed and endorsed by independent stakeholders from major interest groups.

LPCB’s broad range of security protection standards are designed to simulate a variety of circumstances, e.g. in the case of terrorism the likely length of attack, the tools or methods used, or even the likelihood of a stealth attack. Whatever the situation, an effective physical security solution should deter or delay an attacker and should be complimented by a suitable means of detection.

The LPS are always open to revision and should be used for information only. The following product fields are currently covered by BRE’s LPCB scheme:

- Building Products
- Firebreak Doors and Shutters
- Fire Detection and Alarm Systems
- Portable Fire Extinguishers and Fire Hose Reels
- Automatic Sprinkler, Water Spray and Deluge Systems
- Security Systems
- Fixed Fire Fighting Systems
- Smoke and Fire Ventilation Systems.

One example will here be presented in detail to demonstrate how the LPCB standards and other British, European or International standards are used in conjunction to work towards a robust certification of a secure building, where different standards are used for different layers:

Figure 65: BRE/ LPCB layering of standards for a holistic approach to security

As mentioned in the previous chapter, BRE also has a Video Analytics Assessment Programme. Based on the Imagery Library for Intelligent Detection Systems (i-LIDS), the government’s benchmark for video analytics (VA) systems, the British government was responsi-
ble for the certification of such solutions in the past. Since 30 November 2014 BRE has been the authorised test house for the Abandoned Baggage Detection, Parked Vehicle Detection and Doorway Surveillance scenarios as well as evaluations against the Sterile Zone Monitoring Scenario. Although the Video Analytics Programme is regarded as good practice, its focus is on technical issues only. Ethical aspects are not included.

**National Security Inspectorate (NSI)**

The National Security Inspectorate (NSI) is a longstanding certification body for the security and fire industry in the UK. The NSI works on certification for companies and services, not products or systems, and operates a two tier certification systems, which result in either a gold seal or a silver seal.

- **Silver** is designed for ‘Product Certification’ Refers to the ‘Product Certification’ against sector specific standards, e.g. BS 7858, BS 8243.
- **Gold** builds on product Certification to incorporate Quality Management System Certification. The combination of the Quality Management Systems and the relevant sector specific product or service represents the Gold standard of certification. This level holds the greatest perceived value across industry and by the police, fire and rescue services and insurers.”

Source: NSI  
Figure 66: NSI Gold and Silver Certification Seals

NSI cover the following sectors, which are relevant to the CRISP project’s scope:

**Aviation Security**

This auditing was added to the NSI portfolio in 2012 and examines the “application of the QMS (BS EN ISO 9001) to deliver the Department of Transport requirements of SCD No. 1/2010 and incorporate BS EN 10682 for the provision of Airport and Aviation Security Services.”

---

Electronic Security (installation and maintenance)

<table>
<thead>
<tr>
<th>Monitoring and Receiving Centres</th>
<th>Intruder Alarms</th>
<th>Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Receiving Centres</td>
<td>CCTV</td>
<td>Lone Worker</td>
</tr>
</tbody>
</table>

Source: Own figure
Figure 67: NSI solutions in the field of electronic security

NSI offers the NACOSS (National Approval Council for Security Systems) Gold scheme for Electronic Security for which companies must meet standards of business excellence by ISO 9001 Quality Management as well as presenting technical expertise by meeting relevant and appropriate British and European Standards.

For the Silver scheme companies will need to meet high level of technical competence based on the above standards but do not need to meet requirements of ISO 9001.

NSI approves Alarm Receiving Centres (ARCs) with respect to the monitoring of signals received from intruder and fire alarm systems and Remote Video Response Centres (RVRC) for the monitoring of BS 8418 detector activated CCTV systems and other CCTV systems used in security applications.

“All NSI approved ARCs must comply with:

- Approval Criteria
- Technical Standards (BS 5979 and other relevant industry standards)
- Business Standards (covering insurance, premises, finances etc.)
- Codes of Practice (covering industry-specific issues such as customer care)
- Quality Management (complies with ISO 9001 Standard)\textsuperscript{449}"

The following technical standards and codes of practice must be held by a NACOSS Gold or Systems Silver approved companies:

<table>
<thead>
<tr>
<th>Mandatory Standards for all NACOSS holders:</th>
<th>BS 7858:2012 Code of Practice for security screening of personnel employed in a security environment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>BS 7671:2008 Requirement for electrical installations (IET Wiring Regulations) – 17th edition OR the IET On Site guide</td>
</tr>
</tbody>
</table>

**Mandatory Standards for Intruder and Hold-up Alarm Systems**

- PD 6662:2010* Scheme for the application of European standards for intrusion and hold-up alarm systems
- BS 8243:2010 + A1:2014 Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions - Code of Practice
- DD 263:2010 – Intruder and hold-up alarm systems – Commissioning, maintenance and remote support – Code of practice

**Optional Standards depending on work context for Intruder and Hold-up Alarm Systems**

- BS EN 50131 -8:2009 Alarm systems – Intrusion and hold-up systems - Part 8: Security fog device/systems
- BS EN 50136 -1-3:1998 Alarm systems – Alarm transmission systems and equipment - Part 1 - 3: Requirements for systems with digital communicators using the public switched telephone network
- BS EN 50136 -1-4:1998 Alarm systems – Alarm transmission systems and equipment – Part 1-4: Requirements for systems with voice communicators using the public switched telephone network
- BS EN 50136 -1-5:2008 Alarm systems – Alarm transmission systems and equipment – Part 1-5: Requirements for Packet Switched Network PSN
- BS 4737: Section 4.3:1988 Code of Practice for exterior alarm systems
### Mandatory Standards for CCTV Systems

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BS 8418:2010</td>
<td>Installation and remote monitoring of detector activated CCTV systems - Code of practice</td>
</tr>
<tr>
<td>BS 7958:2009</td>
<td>Closed circuit television (CCTV) – Management and operation – Code of practice</td>
</tr>
<tr>
<td>BS 8495:2007</td>
<td>Code of practice for digital CCTV recording systems for the purpose of image export to be used as evidence</td>
</tr>
</tbody>
</table>

### Mandatory Standards for Access Control Systems

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSI Code of Practice NCP 109</td>
<td>for the design, installation and maintenance of access control systems</td>
</tr>
</tbody>
</table>

### Optional Standards for Access Control Systems depending on work and context

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BS EN 50133 -1:1997</td>
<td>Alarm systems - Access control systems for use in security applications - Part 1: System requirements</td>
</tr>
<tr>
<td>BS EN 50133 -7:1999</td>
<td>Alarms systems - Access control systems for use in security applications - Part 7: Application guidelines</td>
</tr>
</tbody>
</table>

### Guarding and Cash Services

NSI offers certification for the following security guarding services:

<table>
<thead>
<tr>
<th>Service</th>
<th>Door supervisors</th>
<th>Aviation security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security guarding and specialised security services</td>
<td>Management and operation of CCTV monitoring schemes</td>
<td>Technical surveillance counter measures</td>
</tr>
<tr>
<td>Keyholding and response services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security screening</td>
<td>Event stewarding and crowd safety services</td>
<td>Private prisons, remand homes, prison escort and court services</td>
</tr>
<tr>
<td>Immigration detention centres</td>
<td>Covert investigation &amp; surveillance</td>
<td>Secure transportation of cash and valuables</td>
</tr>
<tr>
<td>Safe deposit centres</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Own figure  
Figure 68: NSI solutions in the fields of guarding and cash services  

The following standards are used for the certification and evaluation of the above services:
<table>
<thead>
<tr>
<th>Standard Reference Number</th>
<th>Standard title</th>
</tr>
</thead>
<tbody>
<tr>
<td>BS 7858</td>
<td>Code of Practice for Security Screening of Personnel employed in a Security Environment</td>
</tr>
<tr>
<td>BS 7499</td>
<td>Code of Practice for Static site Guarding and Mobile Patrol Services</td>
</tr>
<tr>
<td>BS 7984</td>
<td>Code of Practice for Keyholding and Response Services</td>
</tr>
<tr>
<td>BS 7958</td>
<td>Code of Practice for Closed-circuit Television (CCTV) - Management and operation BS 7960 Code of Practice for Door Supervisors</td>
</tr>
<tr>
<td>BS 8406</td>
<td>Code of Practice for Event Stewarding and Crowd Safety Services</td>
</tr>
<tr>
<td>BS 7872</td>
<td>Code of Practice for Operation of Cash-in-Transit Services (collection &amp; delivery)</td>
</tr>
<tr>
<td>BS EN ISO 9001:2008</td>
<td>Quality Management Systems – Requirements (This standard is used, in addition to the above relevant standards, for those companies who are seeking a gold certification from NSI)</td>
</tr>
<tr>
<td>BS 7984:2008</td>
<td>Keyholding and response services – Code of practice</td>
</tr>
<tr>
<td>BS 8484:2011</td>
<td>Provision of lone worker device (LWD) services – Code of practice</td>
</tr>
</tbody>
</table>

For some approvals the additional NSI codes of practice are also a requirement for certification:

<table>
<thead>
<tr>
<th>Code of practice reference number</th>
<th>Code of practice title</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCP 107</td>
<td>NSI Code of Practice for the Provision of Control Room Services</td>
</tr>
<tr>
<td>NCP 111</td>
<td>NSI Code of Practice for the Provision of Security Screening Services</td>
</tr>
<tr>
<td>NCP 106</td>
<td>NSI Code of Practice for the Management and Operation of Cash Centres</td>
</tr>
</tbody>
</table>

### Fire Detection & Alarm Systems

NSI approves companies through *Fire Gold* and *Fire Silver* schemes to meet the requirements of the BAFE\(^{450}\) SP203-1 Fire Detection and Alarm Systems Scheme. The BAFE Scheme is a third party certification scheme, developed by industry stakeholders and is composed of four modules: System Design, Installation, Commissioning and Handover/Maintenance. NSI approves fire protection companies involved in four sectors:

- Fire detection and alarm systems
- Fixed gaseous fire suppression systems
- Maintenance of portable fire extinguishers
- Emergency lighting

\(^{450}\) British Approval for Fire Equipment
NSI inspects companies to the requirements of the BAFE adopted schemes SP101 and SP203, which are acknowledged by the Fire & Rescue Services, Government, Insurers and the fire industry.

The Approved Contractor Scheme

NSI also certifies in accordance with The Approved Contractor Scheme (ACS) which is designed by the Security Industry Authority (SIA). Its main objective is to raise performance standards in the guarding services sector. By becoming an approved contractor a company must demonstrate that it is competent, well managed and able to deliver a quality service within a number of different areas:

<table>
<thead>
<tr>
<th>Security Guarding</th>
<th>Door Supervisors</th>
<th>CCTV Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Close Protection</td>
<td>Key Holding</td>
<td>Cash/Valuables in Transit</td>
</tr>
<tr>
<td>Vehicle Immobilisation (NI)</td>
<td>Private Investigation (in development)</td>
<td></td>
</tr>
</tbody>
</table>

Figure 69: Areas of the Approved Contractor Scheme

3.9.7. Governmental organisations responsible for conformity assessment in the security field

CESG - The National Technical Authority for Information Assurance

CESG is the national technical authority for information assurance within the UK and is the information security arm of Government Communication Headquarters (GCHQ). CESG deals with the technical aspects of Information Security in Government.

Their activities include:

- “Providing tailored advice to Government on the security risks of new and existing IT systems, and providing ideas and designs to protect those risks
- Building capability through the provision of standards and guidance, working with industry to ensure that appropriately assured products, services and people are available, and
- Building a pool of world class Information Assurance and Cyber Security professionals that organisations can draw upon
- Provide operational support to existing systems by alerting to specific threats and vulnerabilities, providing incident response, and technical solutions such as cryptographic keys to protect the most sensitive information.”

CESG works together with industry and academia and utilises the work of the Centre for Protection of National Infrastructure, MI5 and MI6. Their certification mark certifies that organisations, people, PSS comply with CESG security standards.

---

CESG and its industry partners provide information security services to public and private organisations which aim to reduce vulnerability to cyber-attacks.

**Security Industry Authority (SIA)**

The Security Industry Authority (SIA) was established on the basis of the UK Private Security Industry Act of 2001 to oversee and regulate licencing of the above security practices. “It is a non-departmental public body accountable to the UK Home Office and tasked with the responsibility of regulating the private security industry in England, Wales, Scotland and Northern Ireland.”

SIA now regulates seven sectors of the UK private security industry:

- Security guarding (contract)
- Door supervision (contract and in-house)
- Close protection (contract)
- Cash and valuables in transit (contract)
- Public space surveillance (CCTV) (contract); the immobilisation, restriction and removal of vehicles (contract and in-house)
- Key holding (contract)

The primary objectives of the SIA are:

- To reduce criminality in the private security industry
- To raise standards in the private security industry

The secondary objectives of the SIA are:

- To encourage investment and development in the private security industry;
- To strengthen the ‘extended policing family’ by supporting further engagement with the private security industry

SIA Licencing has focused more on the individuals operating within the private security sector but from 2015 their procedures and scope will also include regulation and licencing of private security businesses. Exact timings regarding the start of the scheme have yet to be

---

confirmed with the Home Office. The scheme however will focus on whether the companies seeking a licence are competent to undertake designated security services it intends to supply. This will be done by determining whether the business conforms to relevant British Standards. The SIA further more stipulates to businesses that the conformity assessment body they choose for their evaluation and must be accredited by the United Kingdom Accreditation Service (UKAS).

In order to receive a business licence from the SIA, security services firms must comply with the following relevant British standards:

<table>
<thead>
<tr>
<th>Standard Reference Number</th>
<th>Standard title</th>
</tr>
</thead>
<tbody>
<tr>
<td>BS 7858</td>
<td>Security screening of individuals employed in a security environment – Code of Practice</td>
</tr>
<tr>
<td>BS 7958:2009</td>
<td>Closed circuit television (CCTV)</td>
</tr>
<tr>
<td>BS 7499:2013</td>
<td>Static site guarding and mobile patrol service. Code of practice</td>
</tr>
<tr>
<td>BS 7960:2005</td>
<td>Door supervisors. Code of practice</td>
</tr>
<tr>
<td>BS 7872:2011</td>
<td>Manned security services. Cash and valuables in transit services (collection and delivery). Code of practice</td>
</tr>
<tr>
<td>BS 7984:2008</td>
<td>Keyholding and response services. Code of practice</td>
</tr>
<tr>
<td>BS 8507-1:2008</td>
<td>Code of practice for close protection services. Services within the United Kingdom</td>
</tr>
</tbody>
</table>

Source: Own figure
Figure 71: Standards which a relevant for receiving business licence for security services in the UK

**Association of Chief Police Officers (ACPO)**

Certification of security systems in the UK differs somewhat from that in the rest of Europe with regard to Police Response to system signals. To gain a police response to an activated alarm, each organisation must adhere to APCO policy, which states:

“To enable a security system to be recognised within the ACPO Requirements for Security Systems it must comply with the ACPO Policy on Police Response to Security Systems and a recognised standard or code of practice controlling manufacture, installation, maintenance and operation. Such standards must be in the public domain and not be product based.

The installation and services provided by the installing company and an Alarm Receiving Centre (ARC) / monitoring / tracking centre (e.g. RVRC, SOC), shall be certified by a United Kingdom Accreditation Service (UKAS) accredited certification body in accordance with the provisions of the ACPO Requirements for Security Systems.  

In order to qualify for police response Alarm Receiving Centres (ARCs), Remote Video Response Centres (RVRCs) and System Operating Centres (SOCs) must comply with standards BS5979 (Cat II) or (BS EN 50518) for Intruder Alarm Monitoring only. At each centre, each system is given a unique reference number (URN).

There are two levels of police response as determined by the ACPO Policy:

- Level One – Immediate response (subject to priorities and resources at the time)
- Level Three – Withdrawn. No police attendance, key holder response only. (Following three false calls in a rolling 12 month period Level 3 will apply and police response will be withdrawn).

To remain on the list of ACPO policy compliant companies, they must:

- Be inspected and recognised by an independent inspectorate body
- Not employ, in surveying, sale, installation, maintenance, monitoring, administration of security systems, individuals with criminal convictions
- Apply and be listed with the home police force where their main office is, before applying to be listed with other police forces
- Take responsibility to update themselves with amendments to the ACPO policy, which is updated each year.\textsuperscript{454}

\textbf{3.9.8. \textit{Summary and Conclusion}}

The British country study showed various interesting aspects. In an effort to increase the speed of standards, the UK has developed the good practice of BSI’s fast track standards: The Public Available Specifications (PAS) and Published Documents (PD), which allow for the establishment of provisional standards that may then be published as full standards if deemed of sufficient quality and fitness for purpose. The Loss Prevention Standards (LPS) offered by Building Research Establishment (BRE) and the ways in which additional requirements are added on to existing standards for certification of security products is also considered a good practice and could potentially be used to respond to additional requirements for specific cases within the CRISP scheme.

The UK also offers interesting examples in several specific areas of CCTV and biometrics in which comparable solutions are missing in many other Member States. The first one is the certification scheme based on the standard iLIDS for CCTV systems and video analytics which was developed by the UK Home Office Centre for Applied Science and Technology. The other interesting solution in the biometric field is offered by the UK National Physical Laboratory NPL. BRE’s Video Analytics Assessment Programme also serves as an example for an outsourcing of security certification functions from the government to private certification bodies. Although the Video Analytics Programme is regarded as good practice, its focus is on technical issues only. Ethical aspects are not included. This shows potential for further research activities.

\textsuperscript{454} Association of Chief Police Officers, op. cit., 2014.
3.9.9. References


BRE, LPCB, Security Systems: Protecting people and property, no date.

http://www.bsia.co.uk/web_images/publications/guarding_benefits_april08.pdf

British Standards Institute and Department for Business, Innovation and Skills, Memorandum of Understanding Between The United Kingdom Government and the British Standards Institution in Respect of its Activities as The United Kingdom's National Standards Body, 2002.


Information Commissioners Office, In the picture: A data protection code of practice for surveillance cameras and personal information, London, 15 October 2014.


http://www.nsi.org.uk/our-services/our-schemes/arcs-rvrcs/

NSI, “Gold and Silver explained”, 2012.


UKTI DSO, UK Defence & Security Export Statistics for 2013, 8 July 2013,

United Kingdom Accreditation Service (UKAS), “About UKAS”, no date.
http://www.ukas.com/about-accreditation/about-ukas/


http://www.sia.homeoffice.gov.uk/Documents/research/sia_baseline_review.pdf
3.10. **The Netherlands**

3.10.1. **Short Description of the Security Industry in the Netherlands**

Within the Netherlands, the main part of the national security industry consists of service providers. Products and systems being used by the service providers are usually developed in other countries.

The largest industry association in the Netherlands is the Dutch Security Association, which represents the private security organisations, criminal investigation organisations as well as organisation which transport money and valuables. The Dutch Security Association represents 90% of the total turnover of the Dutch private security industry (€ 1.38 bn in 2012).\(^\text{455}\)

The Dutch security industry has suffered from the economic crisis over the last years: it has been growing from € 1.07 bn in 2002 up to its highest point in 2008, being € 1.45 bn. After that, the turnover has decreased to the € 1.38 bn in 2012, as mentioned above.\(^\text{456}\) The contraction of the security market is also shown by the decrease of employment. In 2012, 29,390 persons worked in the private security sector, which is 2,153 less than four years before.

The majority of large organisations in need of security (including almost all governmental organisations), obtain those from large multinational security providers. Small and medium organisations obtain their security services from both large and small security service providers. Examples of the multinational security service providers active in the Netherlands are Securitas, G4S and Trigion. The smaller providers vary in size from self-employed entrepreneurs up to organisations with hundreds of employees.

Most organisations in need of security solutions obtain the ‘full package’ at one provider. This means that the security service provider is also responsible for the security products and systems being used. The decision what products and systems are being used is sometimes made by the service provider, but more often this is a decision made by the service provider and client together.

3.10.2. **Security Standardisation Framework**

Almost all standards used in the Netherlands for security products, are standards deriving from the European standardisation organisations CEN and CENELEC and the global standardisation organisation ISO and IEC. The majority of the standards used derive from CENELEC and IEC, being the standardisation organisations focusing on electro technical products. For example, the European standards for alarm systems and CCTV systems are very widely accepted in the Netherlands as being the documents which to rely on, when it comes to the quality of those specific products.

Organisations being active in the national standardisation committee on Alarm systems (which is also responsible for the CCTV standards) are, among others, security service providers, telecom providers, international security products manufacturers and certification

\(^{456}\) Nederlandse Veiligheidsbranche, op. cit., 2013
bodies. Within the European standardisation projects, the Netherlands have a leading role in the standardisation of alarm transmission equipment.

Next to ‘formal’ standardisation which takes place through the national standardisation body NEN and the European and global standardisation organisations, many documents describing requirements to security systems and services are developed by sector organisations or other forums in which organisations gather. For example, within the Dutch Centre for Crime Prevention and Safety and the Dutch Security Association, security service providers and users draft documents which set the minimum requirements to the security services. Within these documents, they refer to NEN/CEN/CELEIEC standards where it comes to the products and systems they use while providing their service.

3.10.3. CONFORMITY ASSESSMENT FRAMEWORK

As in other countries, the conformity assessment framework in the Netherlands consists of certification and accreditation activities.

In the Netherlands, with the law “Wet aanwijzing nationale accreditatie-instantie” (law on the appointment of the national accreditation body) RvA (Raad van Accreditatie) is appointed as the Dutch national accreditation body and is entrusted with the operation of accreditation as a public authority activity within the Netherlands. The RvA is the only national accreditation body and, as such, is a member of the EA and a signatory to the global IAF and ILAC.

The RvA is the only accreditation body in the Netherlands and supervises many certification bodies. In the field of security, there are currently 15 certification bodies which are accredited by the RvA. These 15 certification bodies include bodies certifying products, services or both. They vary from multinational certification bodies like Tüv Rheinland and SGS to local certification bodies. Furthermore, there is a variety in the number of products and services they certify. For example, Tüv Rheinland certifies a very wide range of products, while there are also local certification bodies just certifying one security service. A final division that can be made, lies in the fact that some certification bodies focus solely on the security sector, while other certify products and services in a wide variety of sectors.

Nearly all certification bodies write, use and manage their own certification schemes. This indicates that, even if certification bodies use the same standards and requirements as a basis for their certification activities, the method of testing a product’s or service’s conformity to the standards may vary from one certification body to the other.

3.10.3.1. CERTIFICATION BODIES – OVERVIEW

When searching in the RvA database for certification bodies active in the security sector, 15 certification bodies are mentioned:

• Lloyds Register
• DEKRA Certification
• DNV DL Business Assurance
• IRCLASS Systems and Solutions
• TÜV Rheinland Nederland
• JIC Quality Assurance
• BSI Group The Netherlands
• Ernst & Young CertifyPoint
• GLI Europe
• ControlCase International
• Bureau Veritas Industrial Services
• Telification
• NMi (Netherlands Measurement Institute)
• Brightsight
• Slovenian Institute of Quality and Metrology

However, after consideration of their scope, only few are actually active in the field of security as defined in the scope of CRISP. Most of the certification bodies certify only information security management systems, and not security products, systems or services as the ones being studied within this project.

3.10.3.2. Certification bodies – in depth

Below is an overview of the accredited certification bodies active in the Netherlands, in the security sector as defined in the scope of CRISP.

<table>
<thead>
<tr>
<th>Certification body</th>
<th>Area of certification</th>
<th>Standard used to certify against</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lloyds Register</td>
<td>Security and investigation activities</td>
<td>BS OHSAS 18001</td>
</tr>
<tr>
<td></td>
<td>Public administration and defence; compulsory social security</td>
<td>BS OHSAS 18001</td>
</tr>
<tr>
<td>DEKRA Certification</td>
<td>Security and investigation activities</td>
<td>BS OHSAS 18001</td>
</tr>
<tr>
<td></td>
<td>Public administration and defence; compulsory social security</td>
<td>BS OHSAS 18001</td>
</tr>
<tr>
<td>DNV DL Business Assurance</td>
<td>Security and investigation activities</td>
<td>BS OHSAS 18001</td>
</tr>
<tr>
<td></td>
<td>Public administration and defence; compulsory social security</td>
<td>BS OHSAS 18001</td>
</tr>
<tr>
<td></td>
<td>• Structural provisions;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Technical provisions;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Organisational measures</td>
<td></td>
</tr>
</tbody>
</table>
As shown in the figure above, the accredited certification bodies are mainly active in certification of services, only little in certification of systems and not in certification of products. This can be largely explained by the fact that, as described above, the security market in the Netherlands consists mainly of security service providers. These service providers do use products and systems when performing their services. But since those products are mainly purchased and produced in other countries and manufacturers get their products certified in their own country, there is hardly any security products certification in the Netherlands. This does not mean that the products used in the Netherlands are not certified, it just means that the process of certification does not take place in the Netherlands.

The figure above shows that almost all accredited certification activities rely on standards which are developed by the formal standardisation process, executed by national and international standardisation organisations. BS OHSAS 18001 is a British standard, developed by BSI (British Standards Institute) and accepted internationally. This document has however not been transferred into a European or international standard, but remains a British standard.

The fact that only few certification bodies are accredited to work in the field of security does not automatically mean that there are only few certification activities. Within sector organisations and other forums, certification which is widely accepted, but not formally accredited by the RvA takes place. Although the certification schemes are not accepted by the RvA, the certification process is often executed by certification bodies which are accredited according to general certification standards such as ISO 17021.458

The Dutch security Association manages several quality marks for security service providers, such as event security, general security services and hospitality industry security. These quality marks include requirements regarding integrity, skills of personnel, financial health of the organisation, etc. The certificates are provided by certification bodies such as BSI, SGS and TÜV, all accredited according to ISO 17021. The certification scheme itself however, is not formally accepted by the Dutch Accreditation Council.

458 ISO/IEC 17021:2011 ‘Conformity Assessment – Requirements for bodies providing audit and certification of management systems’
Another example of non-accredited certification are the certification systems, managed by the Dutch Centre for Crime Prevention and Safety (CCV)\(^{459}\). CCV manages different certification schemes, including schemes for fire safety, burglary prevention and private alarm centers. All of these certification schemes are developed and managed by a central committee of experts and certification is executed by accredited certification bodies. The certification scheme for fire safety is (so far) the only scheme which has been accredited by the Dutch Accreditation Council.

3.10.4. **SUMMARY AND CONCLUSIONS**

In the Netherlands, only a small part of certification in the security sector is executed under accreditation. Most of the certification is based on a solid system including certification schemes developed and managed by independent committees of experts, but the schemes themselves are often not accepted by the Accreditation Council. Even without this limitation, the certificates are widely accepted and acknowledged. Therefore, there does not seem to be a strong need to get the schemes accepted by the Accreditation Council.

Especially for the security service providers, there is a wide range of certification systems to choose from. For both the providers and the clients, this fact can lead to confusion. As the chair of the Dutch Security Council, Ms. Laetitia Griffith states in an interview in September 2014, there seems to be a need for closer cooperation between sector organisations ‘to get to preferably one clear quality system for the security sector.’\(^{460}\)

3.10.5. **REFERENCES**


ISO, ISO/IEC 17021:2011 ‘Conformity Assessment – Requirements for bodies providing audit and certification of management systems’


Security Management Magazine, September 2014, pp. 24-26

\(^{459}\) CCV Dutch Centre for Crime Preventio and Safety, Home, no date. http://www.hetccv.nl/english

\(^{460}\) Security Management Magazine, September 2014, pp. 24-26
3.11. **Final remarks on Chapter 3**

Additional talks with industry managers helped to understand the European certification landscape in more detail. An advantage and opportunity is that many internationalized and ‘Europeanized’ certification bodies exist which offer a number of quite identical services in all relevant countries. The problem is that their countries require additional tests against national standards. There are also fields in which standards are missing. Significant differences exist for example with regard to the certification of technical security services. Measures to evaluate the competencies of companies and project managers vary a lot. The new EN 16763 “Services for Fire Safety and Security Systems” from CEN/CLC TC 4 ‘Services for fire safety and security systems’ offers solutions to overcome the problem. Harvey (2014)\(^\text{461}\) developed a concept for further activities. The source suggests a system with three levels to specify the European standards framework of this standard:

- Level 1: EN 16763 plus quality management standards to specify services providers requirements
- Level 2: application guidelines to specify application requirements, supplemented by the comment ‘If not available at European level, national standards may be applied’ and
- Level 3: component standards and systems standards to specify component and system requirements.

Based on this framework, the following approach to enabling service providers to get a certificate for a new country is suggested:

- The entity seeking certification submits all relevant documents with the application.
- The certifier assesses compliance for the works the entity wishes to provide.
- Providing a certificate of compliance with TC 4 requirements issued by another country under the same scheme for the same works would be the basis of proof of TC 4 compliance.
- If there is no certificate provided/available, then the certifier conducts a full assessment to establish TC 4 compliance.
- The certifier conducts a full assessment to establish compliance with country specific laws, regulations and guidelines.

If all steps are successful, then the certificate applied for is issued.

This concepts offers interesting aspects for certification field in which different national requirements hinder the implementation of only one complete and identical certification scheme in all Member States. In addition, it offers specific guidance for the development of solutions for security services.

---

\(^{461}\) Harvey, Martin, *CEN / CENELEC / TC 004* “Services for Fire Safety and Security Systems” EN 16763, presentation May 2014.
### Questions of interviews with representatives of certification bodies

**1. What kinds of products/technologies/systems/services do you test and certify in the security field?**

**2. Please describe your certification process(es) in this area (a chart visualizing the process(es) would be appreciated).**

**3. Which of the following documents form the basis of your testing and certification process(es)?**

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards (please specify)</td>
<td></td>
</tr>
<tr>
<td>Laws/regulations (please specify)</td>
<td></td>
</tr>
<tr>
<td>Internal guidelines/documents (please specify)</td>
<td></td>
</tr>
<tr>
<td>Other (please specify)</td>
<td></td>
</tr>
</tbody>
</table>

**4. Which security products/technologies/systems/services are certified based on the standards mentioned in question 3?**

<table>
<thead>
<tr>
<th>Product/technology/system/service</th>
<th>Standard(s) used in the certification process</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**5. Which security products/technologies/systems/services are certified based on any other documents mentioned in question 3?**

<table>
<thead>
<tr>
<th>Product/technology/system/service</th>
<th>Document(s) used in the certification process</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**6. Do you have a specific quality seal? (If so, please provide a picture/file.)**

**7. What are your key evaluation criteria in the security field and what are minimum requirements for the obtainment of a certificate?**

(please choose three products/technologies/systems/services to answer the question)

<table>
<thead>
<tr>
<th>Product/technology/system/service</th>
<th>Evaluation criterion</th>
<th>Minimum requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product/technology/system/service</th>
<th>Evaluation criterion</th>
<th>Minimum requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
8. Do you cooperate with external test laboratories in the security field? (If so, which ones?)

9. Which institutions are responsible for scenario-based testing of security solutions in your country?

10. Is your organisation involved in security standardisation?
   □ yes (please specify)
   □ no
   □ don’t know

11. How many certificates do you issue annually in the security field? (optional)

12. Are there any (mutual recognition) agreements with other European countries/ certification bodies in the security field?

13. What solutions do you offer suppliers of certified security solutions from other European countries that wish to receive a certificate that is valid in your country?
   [several approaches might exist, depending on the nationality of the producers, the certification system in their home country and the presence or absence of (mutual recognition) agreements]

14. (optional) Are there any other organisations that test and certify security solutions in your country? (If so, please specify)

15. What are current trends with regard to the certification of security solutions from your point of view?

16. Do you have any suggestions regarding the future of testing and certifying security solutions in Europe?

Thank you very much for your time!
4. INTERNATIONAL COUNTRY STUDIES

4.1. UNITED STATES

4.1.1. INTRODUCTION


For several reasons, comparisons with the U.S. are of specific interest for EU research on security standards and certification. In the area of aviation security equipment, the European Commission identified, for example, the following competitive advantages of the U.S. market:

- Lower costs of supplying the market, both in terms of the costs associated with CA and certification of equipment and systems
- Lower uncertainty over the potential market size for new security products and technologies; there is a single U.S. position on the utilisation of technologies and performance standards/requirements.
- Lower risk attached to investments in research, technology development and innovation activities, both because of a more certain market potential and liability situation.
- Shorter ‘time to market’ for new security technologies and innovations.\footnote{More information on the DHS will be provide in chapter 4.1.4.}

The advantages are caused by the fact that only one organisation is responsible for aviation security equipment in the U.S., while each European country has its own responsible organi-
sation is this field. Alarm systems are another example for different requirements in the EU Member States in contrast to the uniform U.S. approach.

This country study provides a comprehensive overview of security standards and certification in the U.S. It shows solutions in the fields of alarm systems, CCTV and services and will also highlight good practice in other market segments.

4.1.2. SHORT DESCRIPTION OF THE COUNTRY’S SECURITY INDUSTRY

The U.S. market for safety and security equipment is the largest worldwide.\(^{467}\) It mainly consists of aviation security, maritime security, border security, critical infrastructure protection, counter terror intelligence, physical security protection and protective closing.\(^{468}\) According to Homeland Security Research,\(^{469}\) the volume of the homeland security market is predicted to be more than $50 bn in 2020.

\[\text{Source: Homeland Security Research}\]
\[\text{Figure 73: U.S. HLS & public safety market (2007-2020)}\]

The long time period, which is covered by Homeland Security Research in Figure 73, also allows comparisons with other reliable sources. Regarding the total security market, the industry association ASIS published a study in 2013, which finds the U.S. security industry to be a $350 billion market.\(^{470}\) This number consists of $282 bn in private sector spending and


\(^{468}\) ECORYS, op. cit., 2009, p. 118.


$69 bn in federal government spending on homeland security.\textsuperscript{471} Operational (non-IT) private security spending was estimated to be $202 bn with expected growth of 5.5 percent in 2013 while the IT-related private security market was estimated at $80 bn with growth of 9 percent projected for 2013.

In contrast to ASIS’s forecast, a number of analyses show that the current demand for security solutions is mainly led by the government (at federal, state and local level). According to ECORYS,\textsuperscript{472} the demand for security equipment has the following structure: U.S. Federal: 60%, U.S. States and local authorities: 10% and U.S. private sector and quasi-governmental: 30%. In contrast, the $282 bn in private sector spending, estimated by ASIS,\textsuperscript{473} represent 81% of the predicted $350 bn market, which shows that ASIS forecasts a substantial increase in private security spending.

A key (governmental) player of the demand side is the DHS, which will be described in more detail in chapter 4.1.4.\textsuperscript{474} Important areas of DHS’s spending include prevention of terrorism and enhancement of security, secure and managed U.S. borders, enforced and administered U.S. immigration laws, safeguarded and secure cyberspace and strengthened national preparedness and resilience.\textsuperscript{475} From a historical perspective, federal funding for homeland security activities has constantly increased since 2006.\textsuperscript{476}

The FY 2016 Budget for the DHS of $41.2 bn in net discretionary funding\textsuperscript{477} includes in particular:

- $3.7 bn for Transportation Security Administration (TSA) screening operations
- Support for U.S. Customs and Border Protection’s Trusted Traveler Programs (no figures given)
- $101 million for Radiological and Nuclear Detection Equipment Acquisition
- $94.5 million for Infrastructure Security Compliance funding to secure America’s high-risk chemical facilities through the systematic regulation, inspection, and enforcement of Chemical Facility Anti-Terrorism Standards
- $86.7 million to enhance White House Complex security
- $83.3 million for the BioWatch Program to provide detection and early warning of the intentional release of select aerosolized biological agents
- $29.4 million for the new Electronic Visa Information Update System and
- $65.8 million for the National Protection and Programs Directorate Replacement Biometric System.

\textsuperscript{471} ASIS, op. cit., 2013.
\textsuperscript{472} ECORYS, op. cit., 2009, p. 49.
\textsuperscript{473} ASIS, op. cit., 2013.
\textsuperscript{476} Masson et al., op. cit., 2011, p. 114-115.
\textsuperscript{477} DHS, op. cit., 2015a, p. 2.
Numerous experts forecast an increase in DHS spending in the years to come with increased funding in some key market sectors such as cyber-security, bio-defense, information technology, Command, Control, Communications and intelligence (C3I), perimeter and border security. Such estimations are, however, questioned by experts who consider that the economic slowdown and the federal budget deficit will have a relevant impact on the budget for security procurement.\(^{478}\)

Regarding the supply side of the market, the five most important companies are Integrated Coast Guard Systems, IBM, Unisys, Fluor Enterprises and Computer Sciences Corporation. In addition, the 20 top U.S. security companies also include the leading military contractors: Boeing, Lockheed Martin, General Dynamics, L3 Com, Northrop Grumman, General Electric, Raytheon, Honeywell, Unisys and SAIC.\(^{479}\) The framework conditions of the companies are described in the following chapters.\(^{480}\)

### 4.1.3. **THE SECURITY STANDARDISATION FRAMEWORK**

#### 4.1.3.1. **THE SECURITY STANDARDISATION SYSTEM IN GENERAL**

The U.S. standardisation infrastructure is regarded as a ‘system that is free from centralized government control but strengthened through essential governmental participation.’\(^{481}\) Most standards are developed and used on a voluntary basis. Standards become mandatory only when included in regulations, codes or contracts for purchase of products. There are four major players/groups of players in the standards development arena, whose work is described in the following:\(^{482}\)

- American National Standards Institute (ANSI)
- National Institute of Standards and Technology (NIST)
- SDOs
- The U.S. government.

According to ECORYS, there are 600 individual standardisation groups and organisations.\(^{483}\) Important players in the security field are described in chapter 4.1.4.

#### American National Standards Institute (ANSI)

ANSI is a non-profit, non-government private-sector membership organisation that is the central focal point for voluntary standards development in the United States. ANSI accredits standards SDOs and approves standards developed by these accredited SDOs as American National Standards (ANS). It also represents and coordinates U.S. positions and interests in international standards development at ISO and the IEC.\(^{484}\) According to an expert, it also

---

\(^{478}\) Masson et al., op. cit., 2011, p. 116.

\(^{479}\) Masson et al., op. cit., 2011, p. 119-121.

\(^{480}\) Masson et al., op. cit., 2011, p. 119-121.


\(^{482}\) The following passages build on ANSI, op. cit., 2013.

\(^{483}\) ECORYS, 2011, op. cit., 172f.

\(^{484}\) ANSI, op. cit., 2013.
coordinates the development of security standards within all accredited SDOs, which are active in that field. These standards have to be developed based on consensus-based processes defined by ANSI.

**National Institute of Standards and Technology (NIST)**

NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. It covers a whole range of services, like weights and measures, calibrations, laboratory accreditation, measurement services and also standardisation. The services are carried out for a broad number of ‘subject areas’: from nanotechnology and bioscience to physics and public safety/security. Together with others, NIST is involved in technical standards, the U.S. CA system, the U.S. accreditation system and the metrology. In this context it is responsible for coordinating federal, state and local activities in voluntary standards and to work with industry and government to develop and apply technology, measurements and standards. See also ECORYS (2011)\(^{485}\) and chapter 4.1.3.3.

**Standards Developing Organisations (SDOs)**

SDOs in the U.S. include ‘professional societies, industry and trade associations and membership organisations’.\(^{486}\) Three types of SDOs can be distinguished in the U.S.:

- SDOs, which submit their standards to ANSI for approval as ANS standards,
- organisations, which develop standards outside the ANSI accreditation and approval process and
- organisations, which develop both kinds of standards depending on the specific framework conditions.

Underwriters Laboratories (UL) provides an example for the last group, not only in the security field. Large SDOs also include ASTM International, IEEE (Institute of Electrical and Electronic Engineers) and ASME International (American Society of Mechanical Engineers). They develop and publish own standards as well as ANSI-approved consensus standards.\(^{487}\)

**Government Agencies**

Almost every agency of the U.S. government has a need for standards for regulation, procurement or operation purposes. The National Technology Transfer and Advancement Act (NTTAA) encourages government agencies to adopt private sector standards and be less dependent on government-unique standards. This practice also reduces the public spending.\(^{488}\)

---

\(^{485}\) ECORYS, 2011, op. cit., p. 173
\(^{486}\) ANSI, op. cit., 2013
\(^{487}\) See ANSI, op. cit., 2013
\(^{488}\) See ANSI, op. cit., 2013
The international dimension

ANSI and U.S. standards developers work with ISO and IEC in the international standards development. ANSI is the sole U.S. representative of ISO. The U.S. National Committee of the IEC (USNC/IEC), a totally integrated committee of ANSI, serves as the focal point for U.S. parties in international electrotechnical standardisation. Figure 7473 shows the U.S. involvement in selected security-related ISO committees.

<table>
<thead>
<tr>
<th>ISO TC</th>
<th>Topic</th>
<th>Participation as P-or O-member</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC/JTC 1/SC 17</td>
<td>Cards and personal identification</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 27</td>
<td>IT Security techniques</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC JTC 1/SC 31</td>
<td>Automatic identification and data capture techniques</td>
<td>P, secretary</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 37</td>
<td>Biometrics</td>
<td>P, secretary</td>
</tr>
<tr>
<td>ISO/TC 85</td>
<td>Nuclear energy, nuclear technologies, and radiological protection</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 92</td>
<td>Fire safety</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 223</td>
<td>Societal security</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 224</td>
<td>Service activities relating to drinking water supply systems and wastewater systems - Quality criteria of the service and performance indicators</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 247</td>
<td>Fraud countermeasures and controls</td>
<td>P, secretary</td>
</tr>
<tr>
<td>ISO/PC 284</td>
<td>Management system for quality of private security company (PSC) operations - Requirements with guidance</td>
<td>P, secretary</td>
</tr>
<tr>
<td>ISO/TC 292</td>
<td>security</td>
<td>-</td>
</tr>
<tr>
<td>Total P+O</td>
<td></td>
<td>10+0</td>
</tr>
</tbody>
</table>

Figure 74: U.S. involvement in selected security-related ISO TCs

According to the figure, a substantial number of the relevant international security TCs are coordinated by an U.S. secretary.

4.1.3.2. RELEVANT LEGISLATION

An important document, which lays the foundation for the American security standardisation framework is the Homeland Security Act 2002, which states that the DHS has to “establish and maintain performance standards (...) and evaluate law enforcement technologies that may be used by, Federal, State, and local law enforcement agencies”. Besides this, it has to
“establish and maintain a program to certify, validate, and mark or otherwise recognize law enforcement technology products that conform to established standards”.⁴⁹⁰ According the Homeland Security Act, these standards should be in accordance with the NTTAA.

Building on the work of Berteau et al.,⁴⁹¹ this chapter also presents selected legislation in America’s key mission areas: counterterrorism, infrastructure protection, preparedness, response and recovery and border security.

**Counterterrorism**

- HSPD–11 Comprehensive Terrorist-Related Screening Procedures, created in 2004, clarifies the terrorist-related screening procedures used by DHS. It calls for coordinated procedures that “detect, identify, track, and interdict people, cargo, and other entities.”⁴⁹²

**Infrastructure Protection⁴⁹³**

- HSPD-7 *Critical Infrastructure Identification, Prioritization and Protection* was released in 2003 for the purpose of developing a framework that “identifies, prioritizes, and protects” the critical infrastructure and key resources⁴⁹⁴ from terrorist attack. It defines the roles and responsibilities of the Secretary, Sector-Specific Agencies, state and local entities, other departments and agencies, as well as the private sector.
- The *Homeland Security Cyber and Physical Infrastructure Protection Act*, introduced in January 2011, enhances domestic preparedness and collective response to terrorist activities by establishing an Office of Cyber-security and Communications. Additionally, this act calls upon the Cyber-security Compliance Division to establish cyber-security requirements for civilian non-military and non-intelligence community federal systems.
- *Executive Order 13636*, “Improving Critical Infrastructure Cybersecurity”, requires NIST to address cyber vulnerabilities “by developing a voluntary framework to

---

⁴⁹³ Critical infrastructure is defined here as “the physical or virtual assets, systems, and networks, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.” Key resources are the “publicly or privately controlled resources essential to the minimal operations of the economy and government,” including agriculture and food, commercial facilities, energy, banking and finance, critical manufacturing, information technology, transportation systems and the defense industrial base.
⁴⁹⁴ Critical infrastructure and key resources
reduce cyber risks to critical infrastructure in a “collaboratively develop[ed] and implement[ed] risk-based” approach.

**Preparedness, Response and Recovery**

- HSPD-8 *National Preparedness of 2003* and the accompanying Annex 1 is a directive designed to enhance the current “preparedness” of the U.S. government’s ability to secure against and/or directly respond to terrorist attacks, natural disasters and sudden emergencies. The fundamental principal of this directive defines the “all-hazards preparedness” goal, which seeks to develop “readiness priorities” and couples the potential and or existing threats with the resources capable of detecting, deterring, and recovering from any national emergencies.
- The *National Response Framework (NRF)* of 2008 provides the framework and guiding principles for the national response architecture and outlines the principles of the response doctrine to better coordinate nation-wide initiatives.
- The Disaster Recovery Improvement Act, introduced in 2011 aims to improve overall disaster relief by expediting the time needed and costs incurred of recovery projects.

**Border Security**

- The *REAL ID Final Rule* released in 2008 established minimal standards for state-issued driver’s licenses and identification cards to standardise state procedures and regulations.

**Aviation and Transportation Security**

- HSPD-11 *Comprehensive Terrorist-Related Screening Procedures Directive*, released in 2004, establishes wide-ranging screening procedures for cargo, people, and other entities suspected and or engaged in terrorist-related activities.
- NSPD-47/HSPD-16, released in 2006, further establish a strategic vision and comprehensive plan for increased border security at all airports and call for the establishment of a National Strategy for Aviation Security.
- The *Secure Airport Terminal Act* of 2011 increases the use of security cameras all airport screening facilities, at both areas of entry and exit. It also requires all cameras be used, maintained and tested in addition to other implemented technologies.

---


496 Direct quote from the relevant document, provided by Hiller and Russell, op. cit., 2015.

Port and Maritime Security

- The *Maritime Port Security Transportation (MSTA) Act* of 2002 provides a strategic framework regulating maritime commerce and the security of domestic sea ports.
- NSPD 41/HSPD13, released in 2004, provides policy guidelines for the U.S. maritime domain and call for the development of a National Strategy for Maritime Security. Released in 2005, this strategy is designed to coordinate and implement all existing Department-level strategies and procedures and security programmes at the State, local, and private sector.
- The *Security and Accountability for every (SAFE) Port Act* of 2006 amends the MSTA, establishes new port facility requirements, calls for the development and implementation of the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-PAT).
- The *Coast Guard Authorization Act for FY2010* establishes a Chief Acquisition Officer to be selected by October 1, 2011. Additionally, it appropriates funds for the establishment of an acquisition directorate designed to supply guidance and oversight for all U.S. Coast Guard acquisition procedures and projects.

One of the major partners for the DHS and the Department of Justice (DOJ) regarding standardisation of security equipment is the National Institute of Standards and Technology (NIST). Based on the Homeland Security Act and the NTTPA, the following sub-chapter will also describe the duties of NIJ, the research, development and evaluation agency of the DOJ.

Another relevant document is the Federal Security Management Act (FISMA) of 2002. More information will also be given in the next sub-chapter.

**4.1.3.3. WORK OF SELECTED STANDARD DEVELOPMENT ORGANISATIONS**

This section represents the work of governmental organisations, SDOs and industry organisations. At the beginning, the work of NIST and the NIJ is presented.

**National Institute of Standards and Technology (NIST)**

Besides the duties mentioned in chapter 4.1.3.1, NIST designs and assists in the implementation of homeland security related CA programmes. It runs several public safety and security programmes, for example:

- X-ray security screening standards for Homeland Security,
- Instrument standards for the detection of hazardous chemical vapours,
- Urban Search and Rescue Robot Performance Standards,
- Metrology and Standards for Canine Olfactory Detection of Explosives,
- Development of NIST Standard Reference Materials for Trace Explosives Detection,
- Measurement Methods and Standards for Public Safety and Security,
- Development of Standard Test Methods for Emergency Response Robots.\(^{498}\)

---

According to Poustourli et al., who refer to the protection of critical infrastructure, NIST standards are particularly relevant in the context of Information Security and Cyber Security. They mention three documents:

- NIST HANDBOOK 150-17 National Voluntary Laboratory Accreditation Program;
- NIST IR 7628 Guidelines for Smart Grid Cyber Security

In 2013 and 2014, NIST also developed a “Framework for Improving Critical Infrastructure Cybersecurity, a Roadmap for Improving Critical Infrastructure Cybersecurity, and a draft of privacy engineering objectives”, which are summarized by Hiller and Russell (2015). Its framework on how to design cyber secure systems addresses the problem of privacy principles, which are currently not integrated into the principles the design of such system. In contrast to the well-known privacy by design concept, it proposes an innovative privacy engineering model.

The NIST Framework offers a “general set of considerations to address privacy concerns as a part of cybersecurity activities.” It also suggest to implement processes to review cyber system defense and response measures for privacy protection.

One of NIST’s duties regarding the design of the cyber security Framework was “to craft definitions and standards for privacy risk management.” In this context ideas for the creation of “privacy engineering along the same lines as security engineering“ arose and NIST started a series of workshops. The first workshop was held in April, 2014 and attracted hundreds of attendees from all stakeholder groups.

The primary objective of the first workshop was “to promote privacy engineering concepts and standardized practices so that system developers could use technical approaches and best practices to protect privacy.” A conclusion of this workshop was, that “Process-oriented principles are an important component of an overall privacy framework, but on their own they do not achieve consistent and measurable results in privacy protection.”

A second workshop took place in September, 2014. NIST presented a draft of Privacy Engineering Objectives and Risk Model (Privacy Framework), as well as a draft of an approach that integrates a privacy risk management framework and privacy engineering elements.

---

500 Hiller and Russell, op. cit., 2015
502 Hiller and Russell, op. cit., 2015
503 Hiller and Russell, op. cit., 2015
504 Hiller and Russell, op. cit., 2015
505 Hiller and Russell, op. cit., 2015
contrast to the focus of the cyber security framework on external privacy risks, the new framework refers to privacy risks within the organisations, which use this concept.

The first privacy engineering objectives are already defined. From the point of the individual user, they include the aspects “predictability, manageability, and confidentiality”. “Problematic data actions” that could undermine those goals were also identified and consist of “appropriation, distortion, induced disclosure, insecurity, surveillance, unanticipated revelation, and unwarranted restriction.”\textsuperscript{508} According to Hiler and Russell, these problematic data actions could lead to privacy harms, defined as “loss of self-determination, discrimination, loss of trust, and economic loss.” While the report of the second workshop is not yet available, Hiller and Russel mention that NIST also gave examples of how specific problematic data actions at different stages of the data life cycle could lead to privacy harms.\textsuperscript{509}

The article also summarises several advantages of the NIST framework: According to the authors, the integration of privacy as a fundamental part of preserving cyber resiliency is perhaps its most important policy concept, since it avoids a choice between privacy and security. The framework also proposes vocabulary that would allow policy and technical sides to “speak the same language.” Built around a risk management model, the Privacy Framework can be applied in “differing contexts, across industries, and internationally.”

NIST also develops FIPS (Federal Information Processing Standards), which are used in the U.S. and Canada. As stated by the Federal Security Management Act (FISMA) of 2002, the U.S. government requires that all products that store or transmit sensitive data, which are intended to be installed in government space, comply with the standard FIPS 140. FIPS 140 is the de-facto standard in the United States and Canada defining security requirements for cryptographic modules that protect sensitive, but unclassified information. It provides a framework for secure design and implementation of products that incorporate encryption methods for data security, integrity, and authentication.

As a general rule, any product that transmits or stores sensitive data can fall under the FIPS 140 umbrella. This includes network hardware such as routers and switches; electronic storage devices such as flash drives and hard drives; wireless devices such as lighting and building controls; smartphones; financial banking tokens; smartcards; and medical devices.

Multiple industry standards rely on FIPS 140 as a basis for data security including the healthcare, energy, information technology, financial, and identity verification industries.\textsuperscript{510} Access to these standards is restricted.

\textsuperscript{508} Hiller and Russell, op. cit., 2015
\textsuperscript{509} Hiler and Russell, op. cit., 2015
NIST CMVP Website \url{http://csrc.nist.gov/groups/STM/cmvp/index.html},
Module Validation List: \url{http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm},
Module-In-Process List: \url{http://csrc.nist.gov/groups/STM/cmvp/inprocess.html},
Cryptographic Algorithm Validation Program: NIST CAVP Website \url{http://csrc.nist.gov/groups/STM/cavp/index.html},
Algorithm Validation Lists: \url{http://csrc.nist.gov/groups/STM/cavp/validation.html},
NIJ is the research, development and evaluation agency of the U.S. Department of Justice.\(^5\) An important aspect of NIJ’s security standardisation activities is the Law Enforcement and Corrections Standards and Testing Programme, which is sponsored by the Office of Science and Technology of NIJ. The programme responds to a mandate of the Homeland Security Act of 2002, which directed the Office of Science and Technology to establish and maintain performance standards in accordance with the NTTAA to test and evaluate law enforcement technologies that may be used by Federal, State, and local law enforcement agencies.

The Homeland Security Act of 2002 also directed the Office of Science and Technology to establish and maintain a programme to certify, validate, and mark or otherwise recognize law enforcement technology products that conform to the standards mentioned above.

The Standards and Testing Program is a research effort that determines the technological needs of justice system agencies, sets minimum performance standards for specific devices, tests commercially available equipment against those standards, and disseminates the standards and the test results to criminal justice agencies nationally and internationally.\(^5\) It operates through:

- The Law Enforcement and Corrections Technology Advisory Council (LECTAC) consisting of nationally recognized criminal justice practitioners, which assesses technological needs and sets priorities for research programmes and items to be evaluated and tested.
- The Office of Law Enforcement Standards (OLES) at the National Institute of Standards and Technology, which develops voluntary national performance standards for compliance testing based on laboratory testing to ensure that individual items of equipment are suitable for use by criminal justice agencies. In addition to the highly technical standards, OLES also produces technical reports and user guidelines that explain in nontechnical terms the capabilities of available equipment.
- The National Law Enforcement and Corrections Technology Center (NLECTC), operated by a grantee, which supervises a national compliance testing programme conducted by independent laboratories. The standards developed by OLES serve as performance benchmarks, against which commercial equipment is measured. The facilities, personnel, and testing capabilities of the independent laboratories are evaluated by OLES prior to testing each item of equipment and OLES helps the NLECTC staff review and analyze data.

Test results are published in Equipment Performance Reports designed to help justice system procurement officials make informed purchasing decisions.\(^5\)

The NIJ created a whole range of security standards in various fields, which are shown in the following figure:

---

\(^5\) Hagy, David, Morgan, John, Caplan, Marc, Stoe, Debra, NIJ, NIJ CBRN Protective Ensemble Certification Program Requirements (draft), 2009
<table>
<thead>
<tr>
<th>Security topic</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Practice for Measurement of Body Armor Wearers Exit(^\text{514})</td>
<td>ASTM E2902</td>
</tr>
<tr>
<td>Public Safety Bomb Suit</td>
<td>NIJ Standard-0117.00</td>
</tr>
<tr>
<td>CBRN Protective Ensemble</td>
<td>NIJ Standard-0116.00</td>
</tr>
<tr>
<td><strong>Detectors</strong></td>
<td></td>
</tr>
<tr>
<td>Portable Bomb X-Ray</td>
<td>NIJ Standard-0603.01</td>
</tr>
<tr>
<td>Handheld Metal Detectors</td>
<td>NIJ Standard-0602.02</td>
</tr>
<tr>
<td>Walk-Through Metal Detectors</td>
<td>NIJ Standard-0601.02</td>
</tr>
<tr>
<td>Drug Reagent Test Kits</td>
<td>NIJ Standard-0604.01</td>
</tr>
<tr>
<td><strong>Tracking</strong></td>
<td></td>
</tr>
<tr>
<td>Vehicle Tracking Devices</td>
<td>NIJ Standard-0223.00M</td>
</tr>
<tr>
<td><strong>Protective Clothing</strong></td>
<td></td>
</tr>
<tr>
<td>Body Armor - Ballistic Resistance</td>
<td>NIJ Standard-0101.06</td>
</tr>
<tr>
<td>Body Armor - Stab Resistance</td>
<td>NIJ Standard-0115.00</td>
</tr>
<tr>
<td>Ballistic Helmets 15, revision underway</td>
<td>NIJ Standard-0106.01</td>
</tr>
<tr>
<td>Protective Gloves</td>
<td>NIJ Test Protocol 99-114</td>
</tr>
<tr>
<td>Ballistic Resistant Protective Materials</td>
<td>NIJ Standard-0108.01</td>
</tr>
<tr>
<td>Riot Helmets and Face Shields</td>
<td>NIJ Standard-0104.02</td>
</tr>
<tr>
<td>Rechargeable Batteries for Personal and Portable Transceivers</td>
<td>NIJ Standard-0211.01</td>
</tr>
<tr>
<td>Hearing Protectors for Use on Firing Ranges</td>
<td>NILECJ-STD-0102.00</td>
</tr>
<tr>
<td>Direct Connect Police Annunciator Panels</td>
<td>NIJ Standard-0320.00</td>
</tr>
</tbody>
</table>

Source: NIJ website, own figure
Figure 75: NIJ standards in the security field

An addition document relevant in the CRISP context is NIJ Guide 101–00 *An Introduction to Biological Agent Detection Equipment for Emergency First Responders.*

The NIJ has a number of ongoing efforts to develop new and update existing standards.\(^\text{515}\) Examples are given below:

The **NIJ Offender Tracking System Standard** will define the minimum requirements and test methods for location and tracking technologies used by law enforcement and corrections officers to monitor and communicate the whereabouts of offenders in all environments within the community.

The NIJ is also developing a performance standard for **vehicular digital multimedia evidence recording systems** (VDMERS) used by law enforcement officers for recording events occurring in and around an enclosed law enforcement vehicles. The standard was written by a

\(^\text{514}\) This standard was produced by ASTM. NIJ staff served on the developing subcommittee.

Special Technical Committee of practitioners, forensic video analysts and testing and certification experts. It addresses video and audio quality, interoperability, safety of operation, environmental resistance and system security.

The development of the **NIJ Electronic Countermeasures (ECM) Standard** is a collaborative effort between NIJ, the FBI, the DHS, the Technical Support Working Group, the National Bomb Squad Commanders Advisory Board, the Joint Counter Radio Controlled Imprisoned Explosive Device Electronic Warfare/Explosives Odnance Disposal JCREW PMS-408 and the Hazardous Devices School.

NIJ is also in the process of revising the **Law Enforcement CBRN Protective Ensemble Standard** based on discussions with the manufacturing community, technical experts and practitioners.

The development of a voluntary **standard for license plate reader (LPR) systems** used by U.S. law enforcement agencies is also noteworthy. The standard is being written by a special TC of local, state, and federal law enforcement practitioners and technical experts.

Finally, NIJ is developing a performance standard for digital **interview room recording systems** (IRRSs) used by U.S. criminal justice practitioners. Such systems are widely used in small and large law enforcement agencies, correctional facilities, detention centers, and jails to record and store digital multimedia evidence from interviews with suspects, witnesses, victims, and others.

In addition to these standards, the NIJ published a Guide for the Selection of Chemical Agent and Toxic Industrial Material Detection Equipment for Emergency First Responders. It provides selection factors and values for chemical detection equipment. A good overview is given on p. 30 of the guide.

Besides NIJ, there is a number of other organisations, which also develop CBRNE related standards. This requires appropriate coordination. A solution is shown in chapter 4.1.3.4. NIJ also offers certification, which is described in chapter 4.1.5.

**Customs Trade Partnership Against Terrorism - C-TPAT**

U.S. security standards for supply chain and container security are developed in a specific way. The U.S. Customs and Border Protection (CBP) set up a public-private partnership (**Customs Trade Partnership Against Terrorism - C-TPAT**), in which public and private actors work together to improve the baseline security standards for the relevant security issues.  

---

516 NIJ, **Selection of Chemical Agent and Toxic Industrial Material Detection Equipment for Emergency First Responders**, Guide 100-00, 2000.

517 ECORYS, 2011a, op. cit., p. 172.
ASTM International

According to its website,518 ASTM International, formerly known as the American Society for Testing and Materials (ASTM), is a globally recognised leader in the development and delivery of international voluntary consensus standards. Today, some 12,000 ASTM standards are used around the world. In particular Committees E12 and E54 are active in the security field.

Committee F12 on Security Systems and Equipment519

Committee F12 has jurisdiction of over 20 standards, and three technical subcommittees. The portfolio of approved standards and Work Items under development are shown below. These standards have and continue to play a preeminent role in all aspects important to security systems, components, and equipment for security of property, life, and product counterfeit protection.

A. Subcommittee F12.10 Systems Products and Services (Physical and Infrastructure Security standards):

- F1642-12 Standard Test Method for Glazing and Glazing Systems Subject to Airblast Loadings
- F2927-12 Standard Test Method for Door Systems Subject to Airblast Loadings
- F2656-07 Standard Test Method for Vehicle Crash Testing of Perimeter Barriers (truck bombs)

B. Subcommittee F12.50 Locking Devices:

- F883-13 Standard Performance Specification for Padlocks

C. Subcommittee F12.60 Controlled Access Security, Search, and Screening Equipment:

- F1448-12 Standard Guide for Selection of Security Technology for Protection Against Counterfeiting, Alteration, Diversion, Duplication, Simulation, and Substitution (CADDSS) of Products or Documents

519 Further information about Committee F12 on Security Systems and Equipment is available on: www.astm.org/COMMITTEE/F12.htm
Committee E54 on Homeland Security Applications

Formed, in 2003, ASTM Committee E54 on Homeland Security Applications addresses issues related to standards and guidance materials for homeland security applications with specific focus on infrastructure protection, decontamination, security controls, threat and vulnerability assessment, and CBRNE sensors and detectors. It is also in charge of the coordination of existing standardisation (ASTM generated as well as external) related to homeland security needs. The Committee currently has its standards published in the Annual Book of ASTM Standards, Volume 15.08. It has the following technical subcommittees:

- E54.01 CBRNE Sensors and Detectors
- E54.02 Emergency Preparedness, Training, and Procedures
- E54.03 Decontamination
- E54.04 Personal Protective Equipment (PPE)
- E54.05 Building and Infrastructure Protection
- E54.06 Electronic Security Systems
- E54.08 Operational Equipment

Regarding privacy, the committee E31.25 on Healthcare Data Management, Security, Confidentiality, and Privacy, a subcommittee of committee E31, is interesting. It published, for example the standard ASTM E1869 Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records.

In addition to the public organisations, there are also several private organisations, initiatives and associations, which develop security standards. Four important players are presented below.

Underwriters Laboratories (UL)

UL is a certification body and an SDO as well, which contributed a substantial number of security documents to the U.S. standards landscape. Numerous UL standards are ANSI approved standards. The following list provides examples in the security field:

- UL 94 Standard for Access Control System Units, May 10, 2013
- UL 68 Smoke Detectors for Fire Alarm Systems, August 14, 2009
- UL 217 Standard for Single and Multiple Station Smoke Alarms, August 25, 2006
- UL 294 Standard for Access Control System Units, January 29, 1999

---

523 E54.04 Personal Protective Equipment (PPE), http://www.astm.org/COMMIT/SUBCOMMIT/E5404.htm
524 E54.05 Building and Infrastructure Protection, http://www.astm.org/COMMIT/SUBCOMMIT/E5405.htm
• UL 365 Standard for Police Station Connected Burglar Alarm Units and Systems, July 31, 1997
• UL 603 Standard for Power Supplies for Use with Burglar-Alarm Systems, February 18, 2008
• UL 609 Standard for Local Burglar Alarm Units and Systems, August 28, 1996
• UL 610 Standard for Central-Station Burglar-Alarm Units, October 26, 1998
• UL 634 Standard for Connectors and Switches for Use with Burglar-Alarm Systems, October 12, 2007
• UL 636 Standard for Holdup Alarm Units and Systems, November 26, 1996
• UL 639 Standard for Intrusion-Detection Units, August 31, 2007
• UL 641 Standard for Installation and Classification of Residential Burglar Alarm Systems, January 26, 2015
• UL 681 Standard for Installation and Classification of Burglar and Holdup Alarm Systems, January 16, 2014
• UL 687 Standard for Burglary-Resistant Safes, July 19, 2011
• UL 827 Standard for Central-Station Alarm Services, June 11, 2008
• UL 864 Standard for Control Units and Accessories for Fire Alarm Systems, December 1, 2014
• UL 1023 Standard for Household Burglar-Alarm System Units, November 25, 1996
• UL 1037 Standard for Antitheft Alarms and Devices, February 24, 1999
• UL 1076 Standard for Proprietary Burglar Alarm Units and Systems, September 29, 1995
• UL 1610 Standard for Central-Station Burglar-Alarm Units, October 26, 1998
• UL 1635 Standard for Digital Alarm Communicator System Units, January 31, 1996

UL also developed a standard with secret content, which is only available for specific stakeholders of security certification, in particular selected persons at security product manufacturers. The development of such standards takes place in a void, which is described by an expert as follows: ‘Some participants are involved in standards development at the consensus level while others are connecting at government to government or agency to agency levels to deal with potential issues. The relevant framework conditions for the development of these standards are defined by the requesters.’ The restricted standard UL 2050 National Industrial Security Systems is used for security certification. More information is given in chapter 4.1.5.2.

The North American Reliability Company

The North American Reliability Company (NERC) is one of the standard-setting organisations responsible for the protection of critical infrastructure and develops standards for the reliability of the bulk power system. It is an accredited body and also responsible for the independent assessments of the reliability and conformity. In addition, it is entitled to impose fines in case of non-compliance.529

529 ECORYS, op. cit., 2011a, p. 172.
National Fire Protection Association (NFPA)

The mission of the NFPA is to reduce the worldwide burden of fire and other hazards on the quality of life by providing and advocating consensus codes and standards, research, training, and education. Originally an U.S. organisation, NFPA has become an international nonprofit organisation and presents itself as ‘the world's leading advocate of fire prevention and an authoritative source on public safety’. NFPA has developed more than 300 consensus codes and standards intended to minimize the possibility and effects of fire and other risks. Its membership totals more than 65,000 individuals around the world. An important NFPA document in the security field is, for example, NFPA 1994 Standard on Protective Ensembles for First Responders to CBRN Terrorism Incidents.

SIBA (Secure Identity & Biometrics Association)

SIBA is a group of companies and other stakeholders that share a common interest in furthering the adoption of secure identity and biometric technologies through forward-thinking thought leadership, and well developed government relations and communications. SIBA white papers provide policy recommendations, technical and factual information, testimony and hearing support, legislative proposals and language.

4.1.3.4. National Strategy for CBRNE Standards

The main aim of the national strategy for chemical, biological, radiological, nuclear, and explosives (CBRNE) standards is to ensure that U.S. emergency response teams on all levels have not only the reliable and necessary equipment in the case of an CBRNE emergency, but also the knowledge and training to handle this kind of emergency. In order to achieve this, the development and implementation of standards is important. The national strategy was established by the National Science and Technology Council Committee on Homeland and National Security, which chartered a subcommittee on standardisation. As one of the main dangers for the national security, “terrorist attack(s) with a weapon of mass destruction” have been outlined as a result of past attacks.

Addressing CBRNE threats was mainly performed on the military basis. The progress in the last years has however shown the necessity of broadening this approach, including especially local first responders like “police, firefighters, emergency medical services, hazardous materials (Hazmat) response units, and bomb squads” into the process of development and implementation of standards. This anticipates the fact that although standardised and tested equipment is essential for the response and management of CBRNE emergencies, this does not ensure that it is also used in a conformant way. The strategy consists of six goals, which

533 National Science and Technology Council Committee on Homeland and National Security, op. cit., 2011
are necessary for standardised and coordinated CBRNE emergency response, including the necessary material.\textsuperscript{534}

**Goal 1: Establish an interagency group for CBRNE standards to promote the coordination of these standards among Federal, State, local and tribal communities.**

A wide range of agencies exist in the USA, which are responsible for the development of standards or research and develop new technologies and equipment, which are necessary for addressing the needs of CBRNE emergency response. Since many of those agencies often develop for their own needs, coordination amongst the existing agencies would promote interoperability between technologies and reduce the duplication of work. That is why the national strategy foresees a single interagency group within the Federal government, which coordinates the development of technology and needed standards. This first goal is essential, since all the other goals rely on the establishment of the interagency group for CBRNE standards.

**Goal 2: Coordinate and facilitate the development of CBRNE equipment performance standards and promote the use of standards for Federal, State, local and tribal communities.**

CBRNE equipment standards might exist already, but since no coordination has been applied so far, many of these standards either do not apply in some areas or are outdated and not applicable anymore. Therefore, the interagency group should assess the current CBRNE equipment performance, in order to identify the gaps and evaluate new and emerging technologies and their significance for CBRNE emergency responses. Like this it will be possible to integrate new technologies at the earliest stage in the standardisation process so that the standards stay up-to-date and “ahead of the technological curve.”\textsuperscript{535} Key characteristics for equipment performance standards, which should be implemented at a minimum level are effectiveness (response time, operating range, etc.), suitability (reliability, availability, interoperability, etc.) and survivability (safety, ruggedness, etc.).

**Goal 3: Coordinate and facilitate the development and adoption of interoperability standards for CBRNE equipment.**

The importance of interoperability of different devices and equipment is also one of the goals of the CBRNE strategy. The communication and information sharing between devices relates largely to the communication interfaces of both the device and the individual, or between the network sensors and the system. Standardisation concerning interoperability has to make sure that functional characteristics like the data output, as well as the physical characteristics (e.g. electrical characteristics), are described in a way that an information exchange between devices is possible. The strategy has identified different devices/equipment in the network of CBRNE emergencies, which require interoperability: “sensors, which report critical data, status, position, alarms, device data integrated with weather, traffic, fire, police and response operations, data provided to responders and decision makers.”\textsuperscript{536} The interoperability also has to make sure that the network of devices is secure.

\textsuperscript{534} National Science and Technology Council Committee on Homeland and National Security, op. cit., 2011, p. 7f.

\textsuperscript{535} National Science and Technology Council Committee on Homeland and National Security, op. cit., 2011, p. 9.

\textsuperscript{536} National Science and Technology Council Committee on Homeland and National Security, op. cit., 2011, p. 12.
Goal 4: Promote enduring CBRNE standard operating procedures for Federal, State, local and tribal use to improve National preparedness and response.
This goal basically sets the requirements for standard operating procedures (SOPs). It refers to the relevant and predictable resources, which are necessary on the strategic, operational and tactical level, to be fully prepared for the coordination of a response in case of a CBRNE emergency. The National Response Framework\(^{537}\) has set a single framework for the emergency response and management of national, large scale incidents. The regular analysis and evaluation of SOPs of CBRNE incidents shall contribute to a harmonisation and improvement of existing SOPs. Standardisation of the mutual procedures is sought.

Goal 5: Establish voluntary CBRNE training and certification standards for the Federal, State, local and tribal communities and promote policies that foster their adoption.
Following goal 4 – the standard operating procedures – the training of in field practitioners and emergency respondents is equally crucial for the effective handling of CBRNE incidents. Several emergency training standards are already available in the USA, but don’t cover every aspect of CBRNE incidents and are also established from different point of views. An analysis of the existing gaps in training standards should thus also be a task of the interagency group, setting standards, in which capabilities of users, trainers, instructors, agencies, are “tightly coupled to standards for operational performance, technical knowledge, and ability to help others increase their capabilities.”\(^{538}\)

Goal 6: Establish a comprehensive CBRNE equipment testing and evaluation (T&E) infrastructure and capability to support CA standards.
Not only training standards are essential for an effective CBRNE emergency response, but also equipment testing and evaluation infrastructure. Due to limited standardisation in the field, several duplications of workflows are present, especially regarding the development of testing facilities, methodologies and performances. There are differences in the equipment of emergency respondents, which influence the testing methodology, but similarities need to be considered regarding the development of principle testing and evaluation standards. The main issues that need to be resolved are the terminology (where different agency use different terms), methodology (different test laboratories have unique methodologies, in some cases also classified), reference material (different standard and regulation references), and certification (different laboratories using different certifications).

These six goals are the core of the National Strategy for CBRNE Standards, and rely thus highly on the interagency group, with its main task of coordinating and harmonising the scattered field of CBRNE emergency preparedness.

4.1.4. THE SECURITY CONFORMITY ASSESSMENT FRAMEWORK

The U.S. security CA framework consists of governmental organisations and private CBs. Important governmental players are the Department of Homeland Security (DHS) as well as the NIJ, the FAA and NIST.

\(^{538}\) National Science and Technology Council Committee on Homeland and National Security, Subcommittee on Standards, op. cit., p. 15.
The DHS was established in 2002 in response to the September 11, 2001, terrorist attacks. It’s goal is to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards. It consists of nine units:

- U.S. Customs and Border Protection (CBP)
- Department of Homeland Security – HQ (DHS-HQ)
- Federal Emergency Management Agency (FEMA)
- Federal Law Enforcement Training Center (FLETC)
- U.S. Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- U.S. Coast Guard (USCG)
- U.S. Citizenship and Immigration Services (USCIS)
- U.S. Secret Service (USSS)

This report will in particular provide information on the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act Office in the DHS Science and Technology Directorate (S&T). Another important player in security certification is the TSA. Both will be described in the detail in the next sub-chapter.

Important private CABs include UL, Intertek, AFFA, ASIS, NICET and SIA. The following figure provides an overview of their services. More information is given in the next chapter.

<table>
<thead>
<tr>
<th>Certification of:</th>
<th>Security products</th>
<th>Security systems</th>
<th>Security services</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Body:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Underwriting Laboratories (UL)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x\textsuperscript{540}</td>
</tr>
<tr>
<td>Intertek</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>AFFA</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASIS</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>NICET</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>SIA</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

Figure 76: Important private security certification bodies in the U.S.

Based on EU Regulation 765/2008, each EU Member State has only one national accreditation body. According to Figure 7776, the U.S. entrusted four organisations with the relevant duties but their accreditations are valid for the whole U.S. market, whose size is comparable with the whole European market for security solutions. This stresses the need to facilitate the framework conditions for CABs and providers of security products, systems and services (PSS), which are active in different EU Member States.


\textsuperscript{540} E.g. materials
Chapter 8 will describe European accreditation issues in more detail and illustrate selected accomplishments of the European cooperation for Accreditation (EA). In addition, it will highlight challenges of CABs with subsidiaries in different Member States and potential solutions for the future.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Logo</td>
<td><img src="image1.png" alt="A2LA Logo" /></td>
<td><img src="image2.png" alt="ANAB Logo" /></td>
<td><img src="image3.png" alt="ANSI Logo" /></td>
<td><img src="image4.png" alt="IAS Logo" /></td>
</tr>
</tbody>
</table>

Source: Own figure based on the websites of the organisations presented above<sup>541</sup>

Figure 77: Accreditation bodies in the U.S.

### 4.1.5. SELECTED SECURITY CERTIFICATION BODIES AND THEIR WORK

#### 4.1.5.1. PUBLIC SECTOR

This section provides information on selected governmental organisations and certification concepts in the U.S. The main focus is put on the SAFETY Act.

---

DHS Office of SAFETY Act

According to its Fact Sheet, the SAFETY Act aims to stimulate the market for security solutions and in particular the supply of anti-terrorism technologies:

‘In the aftermath of the 9/11 attacks, the private sector was extremely reluctant to deploy security technologies and services in civilian settings due to the enormous liability risks involved. Should the company’s technology be impacted by an act of terrorism, the company could be held responsible for any damages. In response, Congress enacted the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act in 2002. (Based on these efforts), the SAFETY Act created liability limitations for claims arising out of, relating to, or resulting from an act of terrorism where Qualified Anti-Terrorism Technologies (QATTs) have been deployed. The Act applies to a broad range of technologies, including products, services, and software, or combinations thereof.’

The SAFETY Act provides for the reduction of liability risks for manufacturers and distributors of anti-terrorism technologies. Further DHS designation and certification under the Act provide de facto approval of security equipment and technologies that is recognised in global markets.

ECORYS summarizes the intended benefit of the SAFETY Act as follows: ‘Given the fact that the U.S. government saw severe positive externalities for innovative (and unproven) security equipment in order to protect the U.S. homeland, they came up with (the SAFETY Act) to solve this market failure.’

Two levels of liability protections, designation and certification exist. According to the following figure, designation can also be obtained for promising anti-terrorism technologies that are undergoing testing and evaluation (Developmental Testing and Evaluation Designations).

---


544 ECORYS op. cit., 2011, p. 174
The DHS describes the parts of the designation and certification concept as follows:

**Designation** means that the seller’s liability for products or services that are deemed “Designated Technologies” is limited to the amount of liability insurance that the DHS determines the Seller must maintain. A **Developmental Testing & Evaluation Designation** may also be obtained for promising anti-terrorism technologies that are undergoing testing and evaluation. In addition to the benefits of Designation, **Certification** allows a seller of anti-terrorism technology to assert the Government Contractor Defense for claims arising from acts of terrorism. Those technologies will be placed on an Approved SAFETY Act Products List for Homeland Security.

---

**Source:** DHS[^545]

Figure 78: Elements of the SAFETY Act

---

Designation is a prerequisite for Certification. The criteria for designation include:

---


https://www.safetyact.gov/pages/homepages/Home.do, p. 6
1. Prior U.S. Government use or demonstrated substantial utility and effectiveness.
2. Availability of the technology for immediate deployment in public and private settings.
3. Existence of extraordinarily large or unquantifiable potential third-party liability risk exposure to the seller or other provider of the technology.
4. Substantial likelihood that the technology will not be deployed unless SAFETY Act risk management protections are extended.
5. Magnitude of risk exposure to the public if the technology is not deployed.
6. Evaluation of scientific studies that can be feasibly conducted to assess the capability of the technology to substantially reduce risks of harm.
7. Effectiveness of the technology in facilitating the defense against acts of terrorism.

In addition, the anti-terrorism technologies must comply to three items: Item C4 ‘Performs as Intended’, Item C5 ‘Conforms to Seller’s Specifications’ and Item C6 ‘Safe for Use as Intended’. According to these items, the seller is required to provide safety and hazard analyses.

The Item C4 ‘Performs as Intended‘ describes the performance-related requirements as follows: Sellers have to ‘explain what it means for their technology to perform as intended and include information demonstrating that the technology will, under reasonable circumstances, consistently perform as intended over time’. If the technology is primarily a device or software product, then the documentation ‘should emphasize the likely operating performance of that device or software’. A demonstration that the ‘technology is effective for its intended use and will perform reliably’ is required. Vendors should provide ‘information regarding the continuing ability of the technology to perform and be used in accordance with specifications’. Examples of such specifications are:

- detection limits,
- mean time between failures,
- probability of detection,
- false positive/negative rates, or
- other metrics.

Relevant information may build on ‘quality control plans, reliability data, evidence of reproducibility between deployments, and evidence that customers can install, use, and maintain the system.’ The solution might also have ‘defined performance specifications that are consistently met while the technology is in operation’.

Vendors of services should ‘provide information on the effectiveness of the core capabilities of the service’. This may build on:

---


548 DHS, op. cit., no date.

549 DHS, op. cit., no date.

550 DHS, op. cit., no date.

551 DHS, op. cit., no date.
sound quality assurance processes,
internal or external auditing services to ensure that the processes remain current,
performance review strategies,
employee screening procedures and certification requirements,
documented practices of updating employee training,
processes for maintaining currency of training and intelligence information, and
similar factors.

If a vendor has successfully deployed his solution or a substantially similar project multiple times with success, then he may provide relevant information as evidence of the performance of his technology. He may, when applicable, demonstrate reproducibility by adherence to well-recognized national or international standards.

**Item C5 ‘Conforms to Seller’s Specifications’** provides support for the claim that the solution ‘conforms (and will continue to conform) to the applicable specifications’. Technical specifications for products should ‘include those items that are invariable from deployment to deployment, such as size, weight, or services provided with the sale of the product (maintenance, warranties, etc.)’

Important aspects are ‘compliance with manufacturing standards, factory acceptance testing procedures, site acceptance testing procedures, quality control processes and procedures, and quality assurance plans’. Government acceptance of the technology and related testing are regarded as highly relevant.

Specifications related to services may refer to ‘the processes and procedures that dictate the implementation of the service. Such processes can be specified in a standard operating procedure document or a process manual.’

**Item C6 ‘Safe for Use as Intended’** requires that the seller conducts and provides safety and hazard analyses for the technology. Such analyses should discuss:

- Documentation pertaining to the safety of the technology.
- Known hazards associated with any part of the lifecycle of the technology.
- Any potential hazards to the seller’s employees.
- Any potential hazards to the purchasers or operators of the technology.
- Any potential hazards to third parties.
- Potential hazards arising from the technology’s deployment in the event of an act of terrorism.
- Potential hazards arising in the event of a false alarm.
- Potential hazards arising from improper deployment, use, or maintenance of the Technology.\(^\text{552}\)

The following figures summarize essential concepts of the SAFETY Act and show the timeline of the relevant application:

---
\(^{552}\) DHS, op. cit., no date.
According to Davidson, the average processing time of a SAFETY Act application was 112.5 days in FY 2013. The DHS approved over 685 applications for SAFETY Act protections including: threat and vulnerability assessment services, detection systems, blast mitigation materials, screening services, sensors and sensor integration, first responder technologies, decision support software, security plans/services, crisis management systems, venue security. It is not required that applicants satisfy all of the relevant criteria to receive SAFETY Act protections.

---


555 Davidson, op. cit., 2014.
protections. In FY 2014, approved technologies generated approximately $3.8 bn in annual technology revenue.

Additional interesting aspects of the concept include the SAFETY Act Block Certification and solutions for experimental technologies.

SAFETY Act Block Certification

The Secretary may issue Block Certifications at his discretion for anti-terrorism technologies that meet established performance standards or defined technical characteristics. Sellers of technologies that are the subject of a Block Certification may submit a streamlined application to be afforded the liability protection available under the SAFETY Act. Block Certification will be published on the SAFETY Act Website (http://www.safetyact.gov). Each Block Certification may set forth particular terms and conditions that should be addressed in the application. 556

Experimental technologies

As described before, designation can also be obtained for promising anti-terrorism technologies that are undergoing testing and evaluation (Developmental Testing and Evaluation Designations, DTED). DTED provide the following benefits to companies.

- Liability = Insurance required by DHS
- Exclusive action in Federal Court
- No Joint and Several Liability for non-economic damages
- No punitive or prejudgment interest
- Recovery reduced by amounts from collateral sources. 557

According to Figure 8079, DTED typically have a term of 3 years and are meant to aid a company’s transition to a full Designation.

Transportation Security Administration (TSA)

The TSA was created to ‘strengthen the security of the nation’s transportation systems and ensure the freedom of movement for people and commerce’. It ‘works closely with transportation, law enforcement and intelligence communities to set the standard for excellence in transportation security.’ 558

The TSA has particular importance in the field of airport screening equipment and is alone responsible for setting the approach to aviation security and technology adoption, for determining performance requirements, for evaluating and approving security equipment and, finally, for the procurement and deployment of equipment. 559 TSA also conducts international

---

557 DHS, SAFETY Act., no date. https://www.safetyact.gov/pages/homepages/SamsStaticPages.do?path=sams\pages\BenefitsToYourCompany.html, see also ECORYS, 2011a, op. cit., 175
aviation security training for countries around the world, focusing on risk-based security strategies, including cargo security, screening techniques, vulnerability assessments and airport security management.\(^{560}\) Certification of civil drones is not done by the TSA but a duty of the Federal Administration Administration FAA, an U.S. Department of Transportation (USDOT or DOT). Originally also part of USDOT, the TSA was moved to the DHS in 2003.

**Federal Aviation Agency (FAA)**

The Federal Aviation Agency FAA is the U.S. aviation authority. It was founded in the context of the Federal Aviation Act in 1958 and has been an administrative part of the Ministry of Transportation since 1966. The major task for the FAA is the issuing of security rules and guidelines for the aviation. This section provides specific insight in the certification of civil drones.

Concerning the certification of UAV-Operations one distinguishes between public operations (special operations of government agencies), civil operations (e.g. commercial operations) and recreational use (private use for recreational reasons). For the latter no authorisation is required as long as the UAV is classified as a model. Public operations are authorised with a COA (Certification of Waiver or Authorization) and are limited to concrete systems, purposes and areas. Civil operations can be certified with SACs (Special Airworthiness Certificates) or COAs and an additional Grant of Exemption complying with section 333.\(^{561}\) A COA is issued in an online process. Two documents have specific importance for the certification of drones: General Regulations described in the Interim Operational Approval Guidance 08-01\(^{562}\) as well as Order 8130.20: Airworthiness Certification of Unmanned Aircraft Systems and Optionally Piloted Aircraft (8.2.2013).\(^{563}\)

**NIST**

NIST, which was introduced in the standards chapter, has been also active in the evaluation of security systems. This section presents specific activities in the biometric and CCTV field. Regarding biometric technologies to improve system and facilities security, the U.S. governments have assisted progress in face-recognition through challenge problems and independent evaluations since 1993, and in iris recognition since 2004.\(^{564}\)

Recently three big projects have been sponsored by six U.S. government organisations: the Face Recognition Grand Challenge (FRGC), the Face Recognition Vendor Test (FRVT) 2006

\(^{560}\) DHS, "Transportation Security Results", 2014c. http://www.dhs.gov/transportation-security-results (Last Published Date: October 31, 2013)


and the Iris Challenge Evaluation (ICE) 2006. The latter provided an independent assessment of diverse iris recognition algorithms on the same dataset, whereas the other projects documented two orders of magnitude improvement in the performance of face recognition under full-frontal, controlled conditions.\(^{565}\)

The Multiple Biometrics Grand Challenge (MBGC) built up on the challenge problems and evaluation and evaluation paradigms of the projects mentioned above but goes further to meet more requirements. The aim is to improve the performance of face and iris recognition technology from biometric samples acquired under unconstrained conditions, both for still images and video.\(^{566}\) MBGC is organised in three challenge problems: The Portal Challenge Problem, The Still Face Challenge Problem and the Video Challenge Problem.

The **Portal Challenge Problem** deals with recognizing people from near-infrared (iris) and high definition (face) video walking through a portal. The availability of both modalities allows for the development of fusion algorithms. The **Still Face Challenge Problem** aims to enhance recognition performance from frontal and off angle still face images taken under uncontrolled indoor and outdoor lighting and to improve recognition performance on still frontal face images that have been resized and compressed. The goal for the **Video Challenge Problem** is to recognize people from video in unconstrained environments.\(^{567}\) The programme has ended, but data are still obtainable for researchers.

**U.S. Department of Justice, Office of Justice Programs, National Institute of Justice**

In general, NIJ administers two testing programmes: (1) standards-based testing and (2) comparative evaluations. These two programmes ensure that the equipment used in the field is safe and reliable and meets the needs of the users.

In the **standards-based testing programme**, products are tested in accordance with voluntary national performance standards. Conducted at NIJ-approved testing laboratories, this testing confirms the equipment's compliance with NIJ standards. Testing of this type is being performed on ballistic-resistant body armor, stab-resistant body armor, metal handcuffs and semiautomatic pistols. Many procurers of public safety agencies require compliance with NIJ standards.

**Comparative evaluation** includes field-testing and publishing test data. Testing of this type is now being performed on patrol vehicles, patrol vehicle tires, replacement brake pads as well as gloves that are cut-, puncture- and pathogen-resistant.\(^{568}\)

The NIJ has also developed the **NIJ Chemical-Biological-Radiological-Nuclear (CBRN) Protective Ensemble Certification Program Requirements**, which determines the certification programme requirements for CBRN protective ensembles for law enforcement. It defines the duties and obligations of the parties involved and the necessary assessment and monitoring.

---


\(^{566}\) Phillips, P. Jonathon, et al., op. cit., p. 2

\(^{567}\) Phillips, P. Jonathon, et al., op. cit., p. 2f

\(^{568}\) NIJ, “Equipment Testing Programs”, 2014, [http://www.nij.gov/topics/technology/standards-testing/Pages/equipment-testing.aspx](http://www.nij.gov/topics/technology/standards-testing/Pages/equipment-testing.aspx)
procedures required to demonstrate initial and continuing compliance with the performance requirements contained in NIJ Standard-0116.00 *NIJ CBRN Protective Ensemble Standard for Law Enforcement*. This document outlines how the CB will plan and conduct initial assessment and surveillance of manufacturers of personal protective equipment in accordance with NIJ Standard-0116.00. It is produced as a part of the NIJ Standards and Testing Program.\(^{569}\)

### 4.1.5.2. Private Certification Bodies

In this sub-chapter important private CBs are presented. UL and Intertek are regarded as the most important CBs for security products in the U.S.

**Underwriters Laboratories (UL)**

UL is an independent safety science company with an international presence. Their services include, in particular, certification, validation, testing, inspection as well as auditing and advisory services. The company provides services for manufacturers and other service providers, including retailers. They provide consultation for governments on global trade initiatives, and collaborate with industry in the development of standards.\(^{570}\) UL is also key player in the U.S. certification landscape for security products, systems and services (PSS),\(^{571}\) which is described in detail in the following sections:

\(^{569}\) Hagy et al., op. cit., 2009.

\(^{570}\) UL, “About UL”, 2015a http://ul.com/aboutul/

\(^{571}\) Statement of an industry expert
### Types of PSS which are tested and certified in the security field

A separate list of all security standards, which UL utilises for certification following the tables shows all types of PSS, for which certification services are provided. Examples for these PSS include:

- Access control
- Alarm services
- ATM security containers
- Baggage scanning equipment
- Ballistic resistant materials
- Biometric devices
- Burglar alarm units and systems
- Central monitoring station receiving units
- CCTV systems
- Hold-up alarm units
- Residential and commercial intrusion detection
- Safes and vaults

In addition to the certification of security PSS, UL is also able to evaluate integrated systems, for example, for fire safety and security as well as combined lighting control and security systems. Certification to the applicable standards ensures, for example, the appropriate handling of different signals and alarms as well as the right priority of signals, depending on whether a signaled incident has an impact on life or personal safety. UL assesses complete control systems to ensure, for example, that a fire alarm has priority and that life-safety-systems are not adversely impacted by other systems.

**Notes:** The certification of CCTV systems includes digital video cameras, where performance is evaluated, such as image quality. UL has also begun a new standards project to determine the appropriate requirements for video used for tactical operations in support of law enforcement and others.

The certification of baggage scanning equipment is conducted in support of the Transportation Security Administration (TSA). This program is intended to address the safety aspects of baggaging scanning equipment (fire, shock and casualty hazards).

### Certification process(es) in the security area

1. Definition of requirements based on criteria in standard(s) applicable to the product type
2. Development of a testing programme based on identified standard(s) and specific constructional features
3. Manufacturer sends a sample of the product or system and the relevant supporting documentation to UL
4. UL performs a construction examination and conducts tests based on the standard(s)
5. The test results are reviewed, a certification decision is made and UL Mark authorization is granted if results are determined to be compliant
6. Manufacturer receives a report with test results and a Follow-up Services (FUS) procedure
7. UL conducts an initial audit/inspection at the manufacturer’s factory(s) and then on a periodic basis
8. Follow-up audits/inspections verify the manufacturer’s capability to produce units that comply with UL requirements and are eligible to bear the UL Mark

The interval of the follow-up inspections depends on the the relative risk involved with the specific products. Generally, life safety and security products undergo more frequent inspections. Modifications to and hardware have to be communicated to UL, who then assesses how themodifications impact the current certification and if additional evaluation/testing is warranted.
### Documents which form the basis of the testing and certification process(es)

<table>
<thead>
<tr>
<th>Standards:</th>
</tr>
</thead>
<tbody>
<tr>
<td>UL uses, in particular, its own, American National Standards Institute (ANSI)-approved standards as well as standards develop by other organisations, such as ASTM (see separate list). Furthermore, UL evaluates products to “multiple safety and performance standards in parallel with FIPS 140 investigations”. Numerous UL standards, including, for example, UL 294 (Access Control Systems) and UL 1610 (Central Station Alarm Systems), reference FIPS 140 for secure communication between devices.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Regulations/laws:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Guidelines of the General Services Administration (GSA), in particular their policy of protection measures around government buildings, for example regarding access control equipment</td>
</tr>
<tr>
<td>• Guidelines of the DHS (while compliance with ANSI standards is regarded as the minimum requirement, additional requirements are, for example, formulated for the certification of baggage screening equipment)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Internal guidelines/documents:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• For specific solutions, new technologies and products for which no standard exists (new standards can be developed. While new standards are developed following the ANSI consensus process, there are some instances where UL develops non-consensus standards where expediency is necessary.)</td>
</tr>
<tr>
<td>• UL may also evaluate features and functionality of products for clients with specific needs that may be more stringent that the minimum requirements of an ANSI standard.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insurance companies, financial institutions and healthcare facilities for example may also have certain requirements beyond the minimum requirements of various security standards.</td>
</tr>
</tbody>
</table>

### Security PSS which are certified based the standards mentioned before

In general, standards are preferred in all areas, in particular consensus-based standards

### Security PSS which are certified based on any other document mentioned before

New and innovative Security PSS can be certified based on new consensus standards or, in some cases, non-consensus standards where expediency is needed. Nevertheless, UL’s preference is to develop consensus standards based on input from all stakeholder groups: manufacturers, integrators of security solutions, installers, the end users as well as the government and academia.

### Certification Mark

According to the overview below, UL has specific Security and Signaling Certification Marks and a simplified product identification for many of the security and signaling product categories.

#### Signaling Mark

The Signaling Mark applies to products such as fire and life-safety alarms. Typical products in this category are smoke detectors, fire alarms and hospital nurse call systems.

---


573. UL, op. cit., 2015b
Security Mark
The Security Mark applies to products such as intrusion detectors, burglar alarms, access controls, anti-theft alarms, surveillance systems, safes and vaults.

Combination Signaling and Security Mark
The Combination Security and Signaling Mark applies to products that serve both security and signaling functions. A typical example is a combination fire and burglar alarm system. Such products are evaluated for both applications.\(^{574}\)

Besides UL’s general marks, these marks signify the certification of specific security functions in addition to product safety in general. Products that perform a security function are evaluated for performance in addition to safety. This is for example important for the certification of cameras to distinguish devices with security functions and devices without such functionalities.

### Key evaluation criteria in the security field and requirements for obtaining a certificate
Currently, in addition to product-specific technical aspects, privacy and data protection are key issues for UL and its clients, for example regarding smart homes, smart building and the Internet of Things. UL has a variety of different standards that address data security aspects and requirements on communication and the encryption of data. They refer for example to data, which is sent from a protected premises and transmitted to a monitoring center. Data security is regarded as a growing certification issue.

An example of UL’s standards, which incorporate data security aspects, is UL 827 for central monitoring stations. It specifies data security requirements which are in line with the NIST cyber security framework. Another example is the UL standard for mass notification, UL 2572. In the context of events such as earthquakes, tornados or other such emergencies, these systems allow the dissemination of advice to people in the affect area, regarding what to do and where to go. UL 2572 incorporates encryption requirements for the relevant information systems to enable secure data transmissions. Requirements around privacy are not included in UL’s current security standards.

Regarding certification in the U.S. in general, the importance of data security aspects in standards for all kinds of critical infrastructure protection, solutions for the protection of water treatment facilities as well as solutions for industrial automation is an important, emerging risk being addressed.

### Field tests
In addition to laboratory tests, UL provides customisable field tests depending on the needs of its customers.

### Certifications issued in the security field annually
Hundreds per year in North America

### Involvement of the organisation in security standardisation
In particular at ANSI. As described earlier, most UL standards are ANSI approved documents.

---

(Mutual recognition) agreements with other countries/CABs in the security field

UL standards and certification are accepted in many countries and regions, such as the Middle East, Asia and Latin America. For example, the Middle East has adopted many UL standards for building materials and life safety. UL strongly believes in harmonised standards and common sets of requirements, toward the ultimate goal to enable manufacturers to develop products that are accepted globally.

Solutions for suppliers of certified security solutions from other countries that wish to receive a certificate that is valid in the U.S.

UL has a process whereby it can consider the testing/testing data and certification work of other organisations. It is able to establish relationships with other organisations which are mutually beneficial by also receiving acceptance of UL’s certification. This is done on a case-by-case basis. The process involves, in particular, the reviewing of the test data and the scope of the certification.

List of standards used by UL for the certification of security PSS

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UL 294</td>
<td>Access Control System Units</td>
</tr>
<tr>
<td>ULC-S319</td>
<td>Electronic Access Control Systems</td>
</tr>
<tr>
<td>UL 294</td>
<td>Access Control System Units</td>
</tr>
<tr>
<td>UL 1610</td>
<td>Central-Station Burglar-Alarm Units</td>
</tr>
<tr>
<td>UL 1635</td>
<td>Digital Alarm Communicator System Units</td>
</tr>
<tr>
<td>ULC-S304</td>
<td>Signal Receiving Centre and Premise Burglar Alarm Control Units</td>
</tr>
<tr>
<td>UL 634</td>
<td>Connectors and Switches for Use with Burglar-Alarm Systems</td>
</tr>
<tr>
<td>ULC/ORD-C634</td>
<td>Guide for the Investigation of Connectors and Switches for Use with Burglar Alarm Systems</td>
</tr>
<tr>
<td>UL 1023</td>
<td>Household Burglar-Alarm System Units</td>
</tr>
<tr>
<td>UL 1610</td>
<td>Central-Station Burglar-Alarm Units</td>
</tr>
<tr>
<td>UL 365</td>
<td>Police Station Connected Burglar Alarm Units and Systems</td>
</tr>
<tr>
<td>UL 464</td>
<td>Audible Signal Appliances</td>
</tr>
<tr>
<td>UL 609</td>
<td>Local Burglar Alarm Units and Systems</td>
</tr>
<tr>
<td>UL 636</td>
<td>Holdup Alarm Units and Systems</td>
</tr>
<tr>
<td>UL 639</td>
<td>Intrusion-Detection Units</td>
</tr>
<tr>
<td>ULC-S306</td>
<td>Intrusion Detection Units</td>
</tr>
<tr>
<td>UL 606</td>
<td>Linings and Screens for Use with Burglar-Alarm Systems</td>
</tr>
<tr>
<td>UL 464</td>
<td>Audible Signal Appliances</td>
</tr>
<tr>
<td>UL 609</td>
<td>Local Burglar Alarm Units and Systems</td>
</tr>
<tr>
<td>ULC-S303</td>
<td>Local Burglar Alarm Units and Systems</td>
</tr>
<tr>
<td>ULC-S525</td>
<td>Audible Signal Devices for Fire Alarm Systems, Including Accessories</td>
</tr>
<tr>
<td>ULC-S303</td>
<td>Local Burglar Alarm Units and Systems</td>
</tr>
<tr>
<td>ULC-S525</td>
<td>Audible Signal Devices for Fire Alarm Systems, Including Accessories</td>
</tr>
<tr>
<td>ULC-S304</td>
<td>Signal Receiving Centre and Premise Burglar Alarm Control Units</td>
</tr>
<tr>
<td>UL 603</td>
<td>Power Supplies for Use with Burglar-Alarm Systems</td>
</tr>
<tr>
<td>ULC-S318</td>
<td>Power Supplies for Burglar Alarm Systems</td>
</tr>
<tr>
<td>UL 1076</td>
<td>Proprietary Burglar Alarm Units and Systems</td>
</tr>
<tr>
<td>ULC/ORD-C1076</td>
<td>Proprietary Burglar Alarm Units and Systems</td>
</tr>
<tr>
<td>UL 1037</td>
<td>Antitheft Alarms and Devices</td>
</tr>
<tr>
<td>ULC/ORD-C1037</td>
<td>Guide for the Investigation of Antitheft Alarms and Devices</td>
</tr>
</tbody>
</table>
D2.2: Consolidated report on security standards and certification

<table>
<thead>
<tr>
<th>Standards</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIJ Standard</td>
<td>Ballistic Resistant Protective Materials</td>
</tr>
<tr>
<td>0108.01</td>
<td>Model Specification for Breath Alcohol Ignition Interlock Devices</td>
</tr>
<tr>
<td>NHTSA</td>
<td>Model Specification for Breath Alcohol Ignition Interlock Devices</td>
</tr>
<tr>
<td>NJI 0101.03</td>
<td>Ballistic Resistance of Police Body Armor</td>
</tr>
<tr>
<td>UL 752</td>
<td>Bullet-Resisting Equipment</td>
</tr>
<tr>
<td>UL 827</td>
<td>Central-Station Alarm Services</td>
</tr>
<tr>
<td>UL 681</td>
<td>Installation and Classification of Burglar and Holdup Alarm Systems</td>
</tr>
<tr>
<td>UL 2050</td>
<td>National Industrial Security Systems</td>
</tr>
<tr>
<td>UL 1635</td>
<td>Digital Alarm Communicator System Units</td>
</tr>
<tr>
<td>UL 1641</td>
<td>Installation and Classification of Residential Burglar Alarm Systems</td>
</tr>
<tr>
<td>UL 365</td>
<td>Police Station Connected Burglar Alarm Units and Systems</td>
</tr>
<tr>
<td>UL 1034</td>
<td>Burglary-Resistant Electric Locking Mechanisms</td>
</tr>
<tr>
<td>UL 972</td>
<td>Burglary Resisting Glazing Material</td>
</tr>
<tr>
<td>ULC-S332</td>
<td>Burglary Resisting Glazing Material</td>
</tr>
<tr>
<td>UL 1981</td>
<td>Central-Station Automation Systems</td>
</tr>
<tr>
<td>ULC-S301</td>
<td>Central and Monitoring Station Burglar Alarm Systems</td>
</tr>
<tr>
<td>ULC-S561</td>
<td>Installation and Services for Fire Signal Receiving Centres and Systems</td>
</tr>
<tr>
<td>BHMA A156.23</td>
<td>Electromagnetic Locks</td>
</tr>
<tr>
<td>UL 305</td>
<td>Panic Hardware</td>
</tr>
<tr>
<td>ULC-S533</td>
<td>Egress Door Securing and Releasing Devices</td>
</tr>
<tr>
<td>ULC-S132</td>
<td>Standard Method of Tests for Emergency Exit and Emergency Fire Exit Hardware</td>
</tr>
<tr>
<td>ULC-S533</td>
<td>Egress Door Securing and Releasing Devices</td>
</tr>
<tr>
<td>ULC-S533</td>
<td>Egress Door Securing and Releasing Devices</td>
</tr>
<tr>
<td>BOCA</td>
<td>National Building Code, Section 1017.4.1.2 Special Locking Arrangements</td>
</tr>
<tr>
<td>BOCA</td>
<td>National Building Code, Section 1017.4.5 Access-Controlled Egress Doors</td>
</tr>
<tr>
<td>Int. Building Code</td>
<td>Section 1008.1.9.6 Special Locking Arrangements</td>
</tr>
<tr>
<td>NFPA 101</td>
<td>Section 7.2.1.6 Life Safety Code</td>
</tr>
<tr>
<td>ULC-S533</td>
<td>Egress Door Securing and Releasing Devices</td>
</tr>
<tr>
<td>ULC-S327</td>
<td>Burglary Resistant Combination Locks</td>
</tr>
<tr>
<td>UL 768</td>
<td>Combination Locks</td>
</tr>
<tr>
<td>UL Subject 2058</td>
<td>Outline of Investigation for High-Security Electronic Locks</td>
</tr>
<tr>
<td>ULC-S334</td>
<td>Burglary Resistant Electronic Combination Locks</td>
</tr>
<tr>
<td>UL 437</td>
<td>Key Locks</td>
</tr>
<tr>
<td>ULC-S328</td>
<td>Burglary Resistant Key Locks</td>
</tr>
<tr>
<td>ULC-S337</td>
<td>Delayed-Action Timelocks</td>
</tr>
<tr>
<td>ULC/ORD-C887</td>
<td>Timelocks</td>
</tr>
<tr>
<td>UL 140</td>
<td>Relocking Devices for Safes and Vaults</td>
</tr>
<tr>
<td>UL 291</td>
<td>Automated Teller Systems</td>
</tr>
<tr>
<td>CSA-C22.2</td>
<td>Safety of Information Technology Equipment, Including Electrical Business Equipment</td>
</tr>
<tr>
<td>No. 950</td>
<td>Safety of Information Technology Equipment, Including Electrical Business Equipment</td>
</tr>
<tr>
<td>UL 687</td>
<td>Burglary-Resistant Safes</td>
</tr>
<tr>
<td>UL 771</td>
<td>Night Depositories</td>
</tr>
<tr>
<td>ULC-S330</td>
<td>Burglary Resistant Night Depositories</td>
</tr>
</tbody>
</table>
In addition to the description of its own activities, UL shared its observation that product development cycles are shrinking and that the market is demanding new products faster. Therefore certification processes and standards development have to become faster and certification organisations need solutions to continuously improve their services and the speed of their processes.

UL also notices a trend towards more performance-based requirements in certification. Regarding the development of advanced security certification services, it highlights the importance of focusing on the security function and the need for standards that are really based on performance. This refers to standards that

- Describe what the intended performance of a product or a system is,
- Specify related requirements and
- Leave it to the industry to determine how to design a solution to meet the specific performance requirement.

In this context, the importance of use cases with different performance levels and security requirements was stressed. Regarding specific solutions, for which performance-based testing is suitable, high security switches employed on doors and windows, for example for intrusion detection was a specific need of the some departments of the U.S. government as well as security containers were mentioned. A specific example was given in the field of CCTV technologies: performance-based requirements enable a broad range of products to be assessed. This is particularly important in the case of CCTV, where a specific use case will dictate the level of performance for a given attribute of a camera.

UL also regards performance-based requirements as a way to keep standards relevant as technologies changes. Therefore, the development of more performance-based, technology neutral requirements and the avoidance of a limited scope on specific technologies are suggested. In addition, the importance of interoperable solutions was highlighted to enable security integrators to develop systems, whose components from different vendors can communicate with each other. In this context, the shift from proprietary solutions to open architecture and the market’s demand for interoperable products was highlighted. UL emphasized the paradigm shift from product-centric devices and systems to integrated systems where security is for example being integrated within fire safety or building management systems. The development of new standards for such systems is expected. UL has realized the need for such as its clients began to request certification for these integrated systems.
Intertek

Intertek Group plc is a multinational inspection, product testing and certification company and a major player in the U.S. security certification landscape. It is an OSHA (Occupational Safety & Health Administration) recognized NRTL (Nationally Recognized Testing Laboratory) and accredited as a Testing Organisation and Certification Body by the Standards Council of Canada. Relevant security products range from all kinds of alarms systems and monitoring companies. Intertek offers various certification marks, including in particular the ETL Mark, which is accepted throughout the U.S. and Canada. Marks, which are relevant in the CRISP context, are shown below:

Source: Intertek
Figure 82: Intertek marks

The ETL Mark is granted to products, which have complied with specific safety or security standards from Europe and North America. Originally created for the Life Safety and Security market in 2005 as an alternative to UL certification, it is ‘one of the certification industry’s most widely known and respected marks’ today.

Among other products, the ETL Mark is used for fire alarms, burglar alarms, smoke detectors and more security systems. The standards, which Intertek tests for North America, are from ASME, ASTM, ANSI, CSA, NFPA, NOM, NSF, UL/ULC.

Intertek has tested the following alarm systems for the U.S. market (in parenthesis are the standards according to which the products were certified): Smoke alarms (CAN/ULC-S531), Single & Multiple Station Smoke Alarms (UL-217), Antitheft Alarms & Devices, Burglar & Holdup Alarm Systems, Burglar, Holdup & Station connected Alarm Services- Police Station connected, Central Station Alarm & Burglar/Holdup Alarm Systems, Fire & Burglar Services, Fire Alarm/Burglar, Holdup & Station connected Alarm Services.

---

578 Canadian Standards Association
579 Norma Oficial Mexicana (Official Mexican Standard)
580 National Sanitation Foundation
An interesting aspect is that Intertek also offers certification of central stations, which represent complex systems of systems. In particular eight documents are pertinent to such certification processes (Figure 82):

<table>
<thead>
<tr>
<th>Standard</th>
<th>Name</th>
<th>Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFPA 72</td>
<td>Nation Fire Alarm and Signaling Code</td>
<td>Application, installation, location, performance, inspection, testing, and maintenance of fire alarm systems, supervising station alarm systems, public emergency alarm reporting systems, fire warning equipment and emergency communication systems (ECS), and their components.</td>
</tr>
<tr>
<td>UL 827</td>
<td>Central-Station Alarm Services</td>
<td>Central-stations providing watchman, fire-alarm, and supervisory services as described in the National Fire Alarm Code, NFPA 72 Central-station burglar-alarm systems intended and specifically designated for burglary protection use at mercantile and banking premises, on mercantile safes and vaults, and on bank safes and vaults Residential monitoring stations monitoring residential alarm systems</td>
</tr>
<tr>
<td>UL 1981</td>
<td>Central-Station Automation Systems</td>
<td>Computerized central-station automation systems intended for use in central-station, proprietary, remote and subsidiary burglar- and fire-alarm applications for the purpose of automating the signal handling and processing of change-of-status signals generated by receivers. In case of failure of an automation system, the receiving equipment is relied on for receiving and recording change-of-status signals and the provision of an audible</td>
</tr>
<tr>
<td>UL 2050</td>
<td>National Industrial Security Systems</td>
<td>Cannot be published - restricted standard, which can be obtained directly through UL</td>
</tr>
<tr>
<td>UL 365</td>
<td>Mercantile and Bank Burglar Alarm System Units</td>
<td>Construction, performance, and maintenance of police station connected burglar alarm units and systems for use in mercantile premises, mercantile safes/vaults, and bank safes/vaults</td>
</tr>
<tr>
<td>UL 1635</td>
<td>Digital Alarm Communicator System Units</td>
<td>Digital alarm communicator system units for use in central-station, proprietary, residential and police station connect burglar alarm systems, residential fire warning systems, and home health care medical alert systems.</td>
</tr>
</tbody>
</table>

---

D2.2: Consolidated report on security standards and certification

### UL 1610
**Central-Station Burglar-Alarm Units**
Components of central-station burglar-alarm systems intended and specifically designated for burglary-protection use at mercantile and banking premises, on mercantile safes, and on bank safes and vaults.

### UL 681
**Installation and Classification of Burglar and Holdup Alarm Systems**
Installation of protective wiring and devices for burglar alarm systems covering premises, stockrooms, closed areas, safes, vaults, night depositories, automated teller machines, and other security containers. The amount of alarm protection installed in a system is designated as extent of protection.

Source: Interek
Figure 83: Standards used for Intertek’s certification of central stations

As shown above, the certificate demonstrates compliance with a substantial number of standards. In addition, Figure 8382 shows that a CB can provide certification based on open standards as well as on standards whose availability is restricted simultaneously. In addition, the relevant standard UL 2050 National Industrial Security Systems shows, that the American CA system offers national standards bodies the opportunity to develop restricted security standards, if necessary.

### 4.1.5.3. **Industry Organisations**

This section presents the programmes of four important industry organisations in the security field: SIA, NICET, AFFA and ASIS.

**Security Industry Association SIA**

The Security Industry Association SIA offers so called CSPM certifications to demonstrate appropriate knowledge for security projects. A Certified Security Project Manager (CSPM®) is “a professional experienced in managing a security project, which typically entails installing and integrating various components of a security system into a physical building structure”. Figure 8483 shows that becoming a CSPM® is a multi-step process.

---

583 SIA, op. cit., no date.
To be eligible for the CSPM® examination, a candidate must have a minimum of 6,000 hours of hands-on project management experience. At least 3,000 hours must have been in direct security project management experience although formal education may substitute for some of the required experience, if necessary.\textsuperscript{584}

The CSPM® exam includes six domains: Security Industry-Specific Knowledge & Initiation, Planning, Execution, Monitoring, Project Closing and Management Skills. Specific examination specifications define the content domains and sub-domains covered on the examination. The examination is comprised of 125 items. Two hours are permitted for the examination.\textsuperscript{585}

More information is provided at SIA’s website. As shown in Figure 8483, the tests are provided in the U.S. and in Canada as well.

**SIA’s Code of Professional Ethics**

In addition to satisfying the educational and experiential requirements, the CSPM® Candidate must agree to abide by the Security Project Manager Code of Professional Ethics to earn the CSPM® certification. The certification holders shall, for example:

- Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character

\textsuperscript{584} SIA, op. cit., no date.
\textsuperscript{585} SIA, op. cit., no date.
• Be accurate and truthful in all dealings with customers
• Serve all members of the public impartially, providing no special privilege or substandard service based upon age, race, national origin, color, gender or handicapping condition.
• Cooperate with SIA concerning ethics violations and the collection of related information.  


**NICET**

The National Institute for Certification in Engineering Technologies (NICET) is the global leader in providing recognition of qualified technology professionals. In the security field, the organisation offers certificates for Video Security Systems Designers and Video Security Systems Technicians.

The **Video Security Systems Designer** programme track includes a sequence of four levels of certification, based on the complexity of the systems being installed/serviced. The content of the four certification builds on three system types: "A", "B", and "C". **Type A Systems** are basic systems with standard components, low bandwidth transmission, and menu-driven setup. **Type B Systems** are systems that can include specialized components, programmable controls, and high-bandwidth transmission while **Type C Systems** are systems that can include PCs, serial communication, and wireless transmission. Certification at a particular level is achieved by demonstrating knowledge of and experience in the work associated with certain types of systems. The four certification levels have the following meaning:

- Level I: in training; assists on Video security systems projects
- Level II: installs type A systems
- Level III: installs types A and B systems
- Level IV: installs types A, B, and C systems

The **Video Security Systems Technician** program offers two testing and certification levels: Level I - Designs Types A and B systems and Level II, which also includes C systems. More information is available at [http://www.nicet.org/](http://www.nicet.org/).

---

586 SIA, op. cit., no date.
587 Such as: Multiplexer/VCR, Quad/VCR, Digital video recorders with time/date, play/record, and anti-tamper functions, Sequential switch, Single keyboard, Indoor/outdoor and Standard cable runs not requiring repeaters or amplifiers (less than 800 ft. for coaxial; less than 1500 ft. for twisted pair)
588 Such as: PTZ, Multiple keyboards, Matrix interfaced with alarms, A/C, or intercom (GPI or dry contact), Digital video recorders with programmable, alarm-based resolution and frame rate, Fiber transmission systems, Low light, Long cable runs, Covert or portable systems and RF modulators.
589 Such as: Integrated systems/serial communications/GUIs, LANs/WANs, Remote systems, Microwave and IR transmission and Digital video recorders with remote interface.
Automatic Fire Alarm Association (AFFA)

NICET certifications are also proposed by the Automatic Fire Alarm Association AFFA and can be passed there, as the organisation wishes to promote and develop “high quality training and educational programs” for personnel. More information is available at http://afaa.org/:

American Society for Industrial Security (ASIS)

ASIS International is the leading organisation for security professionals, with more than 38,000 members worldwide. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programmes and materials that address broad security interests. ASIS also advocates the role and value of the security management profession to business, the media, government entities, and the public. As ANSI-accredited SDO, ASIS works with national and international standards-setting organisations to advance security practices worldwide through the development of standards and guidelines within a voluntary, non-proprietary and consensus-based process. The organisation administers three internationally accredited certifications: the Certified Protection Professional (CPP), Professional Certified Investigator (PCI), and the Physical Security Professional (PSP):

Certified Protection Professionals (CPP)® demonstrated knowledge and experience in all areas of security management. Eligibility requirements include nine years of security work experience, with at least three of those years in responsible charge of a security function or a bachelor's degree or higher and seven years of security work experience, with at least three of those years in responsible charge of a security function. The exam consists of 200 scored multiple-choice questions plus 25 ‘pre-test’ (unscored) questions. The exam domains include Security Principles and Practices (19%), Business Principles and Practices (11%), Investigations (10%), Personnel Security (12%), Physical Security (25%), Information Security (8%), Crisis Management (8%) and Legal Aspects (7%).

Professional Certified Investigators (PCI)® demonstrated education and/or experience in the fields of case management, evidence collection, and case presentation. The eligibility requirement is a high school diploma or equivalent and five years of investigations experience with at least two years in case management. The PCI examination consists of 125 multiple-choice questions plus 15 ‘pre-test’ questions. PCI exam domains include Case Management (29%), Investigative Techniques and Procedures (50%) and Case Presentation (21%). The certification is applicable to a wide range of specialised investigations including:

- arson
- forensics
- high-tech crime
- narcotics
- workplace violence
- child abuse
- gaming
- insurance fraud
- property & casualty
- economic crime
- health care fraud
- loss prevention
- threat assessment

590 According to ASIS, case management is ‘the coordination and direction of an investigation utilizing various disciplines and resources, the findings of which would be assessed to establish the facts/findings of the investigation as a whole; the management process of investigation’
Physical Security Professionals (PSP)® demonstrated experience in physical security assessment, the application, design and integration of physical security systems, and implementation of physical security measures. Eligibility Requirements are a High school diploma, GED equivalent, or an associate degree and six years of progressive physical security experience or at least a Bachelor's degree plus four years of progressive physical security experience. The exam consists of 125 multiple-choice questions plus 15 ‘pre-test’ (unscored) questions. PSP Exam Domains include Physical Security Assessment (33%), Application, Design, and Integration of Physical Security Systems (38%) and Implementation of Physical Security Measures (29%).

4.1.6. SUMMARY AND CONCLUSION

Being the largest market for security solutions worldwide, the United States offers strong examples of good practices and provides working models of advanced security measures for further study (see CRISP WP 3 and WP 4). One particular quality that will be essential to the development of a harmonised pan-European security certificate will be collaboration between a large number of agencies. The National Strategy for CBRNE Standards, which was developed in response to coordination issues between various organisations, can serve as an example upon which CRISP can base future efforts in response to the need to promote and sustain collaboration between the 28 EU Member States.

Other important security sector standards and certifications, which are considered good practice include: the SAFETY Act, which applies to a wide range of technologies, including products, services as well as software and other forms of intellectual property, making it suitable for many kinds of security solutions. In addition, it offers Developmental Testing and Evaluation Designations for experimental technologies; the National Technology Transfer and Advancement Act (NTTAA) that encourages government agencies to adopt private sector standards and be less dependent on government-unique standards, thereby reducing the cost of government operations; SIA’s Code of Professional Ethics which provides an example for the inclusion of ethical aspects in security-related certification; Federal Information Processing Standards (FIPS), that deals with the processing of sensitive data; and the private CB UL responsible for the private certification of metal detectors. Contrastingly, other security schemes vary greatly in terms of the necessary experience and the content of the tests and certificates, which European efforts towards standardisation will discourage, enabling Europe to develop a competitive advantage in this regard.

The existence of both the UL security seal and the Intertek mark, available in Canada and in the United States, was also found to support competition, which discourages monopolistic market conditions and promotes transparency and coexistences. According to an industry expert, “Competition is good in any case. It usually improves processes (leading to faster procedures and thus faster time to market) and also reduces costs. Of course, the certification rules must be identical. This is ensured in the case of UL/Intertek. From the industry point of view, a pan-European security certificate, which avoids a monopolistic position and can be received

591 Physical security is defined as the various physical measures designed to safeguard personnel, property, and information. Progressive means that the experience has included increasingly more difficult assignments or responsibilities over the work period
593 ECORYS, op. cit., 2009, p. 47.
at different institutions based on the same requirements, is also desirable.” Moreover, the existence of two strong coalitions working towards common standards raises the trust of stakeholders – something that will be fundamental in European efforts to further expand the security industry, while including already existing coalitions, both goals of CRISP certification.

However, Europe has specific challenges not present in the United States. According to the same industry expert referenced above, ‘Intertek entered the same market as UL. Unlike the European market for security solutions, this North American market is homogeneous. A pan-European certification scheme has to cope with all local rules and languages and has to compete with many country-specific leaders of the market for security certificates. This is much more difficult’.

The country study of the United States also provides information on the development and use of restricted standards by standards and CBs. Collecting more information in this regard is suggested, in particular to analyse the processes to create and use these standards. Furthermore, shrinking product development cycles are needed for faster certification processes and standards development. An emphasis on the importance of performance-based requirements and of use cases for standardisation and certification should be made and the need for interoperable solutions and paradigm shifts from product-centric security devices and systems to integrated systems, which define a new demand for specific standards, should be further examined.

4.1.7. REFERENCES


Cavoukian, A., “Privacy by Design. The 7 Foundational Principles“. 

Davidson, Bruce, 2014 Regional Meeting (Regions 9 and 10) Protective Security Advisor Program Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act, July 30, 2014. 


DHS, “Transportation Security Results“, 2014c. 
http://www.dhs.gov/transportation-security-results

DHS, “DHS Form 10004 (10/06)“, 2006. 
https://www.safetyact.gov/jsp/attachment/samsAttachmentDownload.do?action=getStreamInfo&attachmentId=9&fileName=10004_SAFETY_Act_Block_Certification%202_.pdf

DHS, “Application for SAFETY Act Certification”, DHS Form 10007, no date. 
https://www.safetyact.gov/jsp/attachment/samsAttachmentDownload.do?action=getStreamInfo&attachmentId=5&fileName=10007_Application_for_SAFETY_Act_Certification.pdf


E54.02 Emergency Preparedness, Training, and Procedures, 
http://www.astm.org/COMMIT/SUBCOMMIT/E5402.htm

E54.03 Decontamination, 
http://www.astm.org/COMMIT/SUBCOMMIT/E5403.htm

E54.04 Personal Protective Equipment (PPE), 
http://www.astm.org/COMMIT/SUBCOMMIT/E5404.htm

E54.05 Building and Infrastructure Protection, 
http://www.astm.org/COMMIT/SUBCOMMIT/E5405.htm

E54.06 Electronic Security Systems,
E54.08 Operational Equipment,
http://www.astm.org/COMMIT/SUBCOMMIT/E5408.htm


Hagy, David, Morgan, John, Caplan, Marc, Stoe, Debra, NIJ, NIJ CBRN Protective Ensemble Certification Program Requirements (draft), 2009


4.2. **CANADA**

4.2.1. **INTRODUCTION**

The focus of this chapter is to present analysis of the state of the art in standards and certification in Canada. The country’s security industry, the standardisation framework and the security framework are analysed. In addition, selected security CBs and their work are described. Finally, a comparison between Canadian and the European accreditation and certification framework is provided.

4.2.2. **SHORT DESCRIPTION OF THE COUNTRY’S SECURITY INDUSTRY**

The increasing importance of security has generated new challenges for the Canadian government. The commitment of the Canadian stakeholders to the security of its citizens has stimulated a large demand for security PSS since new and high-end technologies have endangered their security. New, or updated, security standards have been developed to provide leading-edge security solutions to suit the current social, economic and political circumstances.

The Canadian security market is mostly made up of governmental entities (i.e. Royal Canadian Mounted Police (RCMP), Canada Border Services Agency (CBSA), Correctional Services Canada (CSC), Ontario Provincial Police (OPP) and other municipal police services). Together with the Department of National Defence (DND), they spent close to US$ 8 bn on security and defense in 2011. Thereof 75% were domestic expenditures and 25% foreign. In general, the Canadian Security and Safety Industry is an open and transparent market with about 2,000 competitors directly involved.

The market is facing increasing demand given the growing role of security in day-to-day business operations. One field that is evolving especially strong is *Cyber Security*. Both governmental institutions and private corporations have repeatedly been the target of cyber-attacks with growing frequency and sophistication. Therefore cyber criminality is considered as a mayor threat. This is also reflected in an extended budget for Cyber Security. Within five years the Canadian Cyber Security Budget was doubled to US$ 245 million.

The demand for security products and services to protect commercial buildings and facilities was expected to grow by 1 or 2 % yearly over a period of 20 years. Other fields of interest for Canada are arctic management, environmental safety, protection of sovereign interests in the North and emergency preparedness for natural disasters.

---


4.2.3. **The Standardisation and Accreditation Process**

Nowadays, an important task facing governments, private organisations, consumers and users is to develop effective and efficient accreditation and certification systems. In Canada, this system takes its mandate from the Standards Council of Canada Act. The Standards Council of Canada (SCC) is Canada’s national accreditation body, which accredited the four national SDOs.

- a) The Canadian Standards Association Group (CSA).
- b) Underwriters Laboratories (UL).
- c) Canadian General Standards Board (CGSB).
- d) Bureau de normalisation du Québec (BNQ).

A tri-harmonized committee composed by CGSB, ULC and CSA is developing international standards in the security area. BNQ has no security standards and exclusively provides certification in the field of explosives (CAN/BNQ 2910-500).

The CSA and UL are private organisations covering a wide variety of commercial goods and services. The CGSB and BNQ cover areas related to the activities of the Canadian federal and Quebec provincial government respectively. Each of these organisations develops standards through committees representing various interests.

Every SDO has been given the responsibility for their subject area, although currently the field has been opened up recently to the American Society for Industrial Security (ASIS). In this process, a professional project manager is provided by the SDO and subject matter experts are identified to give their knowledge on the issue. A volunteer TC of subject matter experts is assembled. Stakeholders such as the government, experts, consumers, and developers may participate in the meetings. Finally, the TC set a draft reviewed by these stakeholders reflecting in this way the breath of the Canadian society.

To receive approval, a standard must be developed by an SCC-accredited SDO and submitted to SCC, which may approve it as a National Standard of Canada (hereinafter, NSC) based on

---

597 The Standards Council of Canada (SCC) is a federal Crown corporation that coordinates standardisation activities in Canada. It is regulated in Subsection 4. (1), Standards Council of Canada Act, R.S., 1985, c. S-16, s. 5; 1996, c. 24, s. 4; 2011, c. 21, s.156, amended March 16, 2012. It is independent of governmental interests, although it is financed by public funds. The SCC does not develop standards itself, nor does it conduct any conformity assessments. Standards Council of Canada Act (R.S.C., 1985, c. S-16) is available on: http://laws-lois.justice.gc.ca/eng/acts/S-16/page-1.html


599 All SCC-accredited SDOs have met the same requirements in order to receive SCC accreditation.

600 ISO/TC 292 develops international standards in the field of security, including but not limited to general security management, business continuity management, resilience and emergency management, fraud countermeasures and controls, security services, homeland security.


603 Up until now, there have not been problems of unifying similar standards since each SDO has had certain areas of expertise, which did not overlap with any of the other Canadian SDOs. However, this might change, since ASIS has a business continuity standard developed jointly with BSI (ASIS/BSI BCM.01-2012), but there is already a Canadian National Standard (CSA Z1600-14).
a specific set of requirements in the specific subject area. Subsequently, NSC must be published as a CAN-P on the SCC’s website in order to come into effect before the stakeholders. In addition, every SDO shall publish its CAN-Ps developed.

SDOs are also responsible for the maintenance of any NSC they publish and must review the NSC within five years of its development. Also, SDOs seeking accreditation to SCC’s Standards Development Program must comply with CAN-P-15 and CAN-P-1020. SCC-accredited SDOs are coordinated in order to avoid duplication within the Canadian standards development environment and to promote opportunities for harmonization wherever possible.

As a condition of maintaining accreditation, CAN-P-1020:2013 defines specific requirements: if the requirements for accreditation change, SDOs shall demonstrate compliance with the new requirements. Apart from that, SDOs shall notify to SCC of any changes to their policies and procedures as they occur. In addition, SCC may also request a retirement if it determines a standard no longer meets the requirements established in CAN-P-2. In both cases, SCC shall take appropriate measures and inform the public of the change.

An additional international SDO is ASTM International. Information on ASTM International standards in the area of security are provided in the country study “United States”.

4.2.4. THE SECURITY STANDARDISATION FRAMEWORK

In Canada, the design, testing or analyses of standards are a liberalised activity. Public (e.g. government representatives, public researchers institutes) but also private bodies (e.g. consumers, users, manufacturers, contractors, engineers, architects and other experts) may create

---

604 If the standard become in a NSC, must have complied with the following requirements: it must have been developed by consensus of stakeholders; subjected to public scrutiny; published in both official languages in order to comply with the principle of publicity; consistent and focus on facilitating international market. In addition, SDOs (applicants) must meet the requirements laid down in CAN-P-1. https://www.scc.ca/en/about-scc/publications/criteria-and-procedures/can-p-1020-2013-program-requirements-sdo

605 CAN-P-15 – Policy for the Suspension and Withdrawal of Accreditations and the Resolution of Complaints and Appeals ensures that the result of such actions can be objectively and impartially challenged and investigated.

On the other hand, CAN-P-1020 - Program Requirements for SDO Accreditation to CAN-P-1 requires a set of requirements throughout the term of the standard (eligibility, granting of accreditation, changes in requirements and changes in SDO Policies and procedures). Canadian Standards Development Program Requirements for SDO. Accreditation to CAN-P-1. https://www.scc.ca/en/about-scc/publications/criteria-and-procedures/can-p-1020-2013-program-requirements-sdo

606 The CAN-P-1:2012 4.3 states: “An important facet of the Canadian standards development system is to avoid duplication of standards while demonstrating respect for the Canadian concept of subject area recognition of responsibility.”

607 CAN-P-1020: 2013 - Program Requirements for SDO Accreditation to CAN-P-1 - May 2013. 4. General requirements. 4.3 Changes in requirements: If the requirements for accreditation change, SDO’s shall demonstrate compliance with the new requirements of CAN-P-1 as a condition of maintaining accreditation. A phase in period will be determined by the SCC. This period shall be notified to the SDO’s. 4.4 Changes in SDO Policies and procedures: The SDO shall identify and inform SCC of any changes to their policies and procedures as they occur. https://www.scc.ca/sites/default/files/publications/CAN-P-1020-2013_e.pdf

608 Standards Council of Canada, “Requirements and Procedures for the Request for, Development, Approval, Preparation, and Maintenance of National Standards of Canada” p. 12, states the following regarding to CAN-P2F: “NSC status shall remain in effect as long as the standard continues to meet all established requirements. An SDO, judging that its standard fails to meet any requirement, must inform the SCC and request that the NSC status be removed by the SCC. Upon receipt of that information, the SCC shall take appropriate measures and inform the public of the change. The SCC may also request a withdrawal if it determines a standard no longer meets the requirements of CAN-P-2. The SDO may resubmit the standard for approval after having taken corrective action such that all the requirements are met”. https://www.scc.ca/sites/default/files/liferay_files/CAN-P-2F_e.pdf
standards according to their knowledge on a specific issue. SCC also identifies or responds to a request/need for a new area of standardisation.\textsuperscript{609}

**Standards Council of Canada (SCC)**

Standards Council of Canada Act (SCC)\textsuperscript{610} regulates the standardisation process in Canada. It establishes the SCC as a crown corporation to promote and encourage efficient and effective voluntary standardisation in Canada.

In 2000, The Canadian Standards Strategy was launched the strategy provided direction and leadership on how to use standardisation to advance the social and economic well being of Canadians.\textsuperscript{611} To achieve this, it was published the Canada Gazette in 2002\textsuperscript{612} in order to expand the list of countries, in which the SCC could accredit CA organisations. Finally, SCC launched the Canadian Standards Strategy Update: 2005-2008.\textsuperscript{613}

The structure of the SCC according to Article 3 of Standards Council of Canada Act includes:

- The Chairperson and Vice-Chairperson of the Provincial-Territorial Advisory Committee established under subsection 20(1): are a non-voting members of the Council (art. 6.3)
- The Chairperson of the SDOs’ Advisory Committee established under subsection 21(1); and
- Not more than 10 other persons to represent the private sector, including non-governmental organisations.

According to Article 6.2 of the above-mentioned Act, the protection of interests in the private sector is the main purpose of these members. In addition, they are required to have the knowledge or experience necessary to assist the Council in the fulfilment of its mandate.

The SCC leads and facilitates the development and use of national and international standards and accreditation services in order to enhance Canada's competitiveness and well-being.\textsuperscript{614} In essence, the SCC provides\textsuperscript{615} is the following:

- Promoting efficient and effective voluntary standardisation in Canada.
- Supporting sustainable development, benefit the health, safety and welfare of workers and the public.
- Assisting and protecting consumers.

\textsuperscript{609} Canada's National Standards Framework includes more than 400 organizations accredited by the SCC. These organizations are involved in several activities, such as: standards development, product testing and quality (conformity assessment), product or service certification, and environmental management and production systems registration.

\textsuperscript{610} Further information about SCC is available at: Government of Canada, Justice Laws Website, “Table of Contents” 04.06.2015 http://laws-lois.justice.gc.ca/eng/acts/S-16/

\textsuperscript{611} Its recommendations continue to underpin SCC plans and strategies.

\textsuperscript{612} The list now includes countries that are members of the World Trade Organization.

\textsuperscript{613} Further information about SCC history available on: https://www.scc.ca/en/about-scc/history

\textsuperscript{614} Information available on SCC’s website: https://www.scc.ca/en/about-scc/mandate-mission-vision

\textsuperscript{615} According to Subsection 4. (1), Standards Council of Canada Act, R.S., 1985, c. S-16, s. 5; 1996, c. 24, s. 4; 2011, c. 21, s.156, amended March 16, 2012.
• Facilitating domestic and international trade, and further international co-operation in relation to standardisation.
• Serving as the government’s focal point for voluntary standardisation.
• Representing Canada in international standardisation activities, setting out policies and procedures for the development of National Standards of Canada.
• Offering several programmes for the accreditation of CABs and SDOs.
• Fostering and supporting the principle of recognition of CA results and equivalent systems as a means of decreasing multiple assessments and audits, both in Canada and with Canada’s trading partners.

**Canadian Standards Association (CSA Group)**

CSA is a non-profit association that promotes efficient and effective standardisation processes in Canada, serving business, industry, government and consumers nationally and in the global marketplace in more than 50 areas of technology, including new technologies. It was established as the Canadian Engineering Standards Association (CESA) in 1919 although in 1950 changed its name to the Canadian Standards Association (CSA). Its certification mark, currently applied on products globally, was established and became a member of the ISO.

CSA has no security standards for equipment but publishes the software standards of ISO/IEC JTC1\(^{616}\) as Canadian adoptions. Nevertheless, there are no testing or certification services they supply for the ISO/IEC JTC1 standards. If someone wants to be certified, CSA may study the request according to the specific needs in the market.

In their accreditation CSA shows a general category for security but in their listings there are very few (i.e. CAN/CSA-Z246.1-13: Security management for petroleum and natural gas industry systems).\(^{617}\)

At this time CSA Group is not directly involved in the standardisation of security products. Its only involvement has been:

• Serving as the national standards body for adoption of the ISO/IEC JTC 1 standards on information technology (adopted in Canada with no national deviations) some of which deal with software security, and
• Supporting Canadian participation in the ISO work in the TC 292 on security.

---

\(^{616}\) ISO/IEC JTC1: International standardisation in the field of Information Technology. Information Technology includes the specification, design and development of systems and tools dealing with the capture, representation, processing, security, transfer, interchange, presentation, management, organization, storage and retrieval of information. JTC 1 is the standards development environment where experts come together to develop worldwide Information and Communication Technologies (ICT) standards for business and consumer applications. Additionally, JTC 1 provides the standards approval environment for integrating diverse and complex ICT technologies. These standards rely upon the core infrastructure technologies developed by JTC 1 centres of expertise complemented by specifications developed in other organizations.

\(^{617}\) CAN/CSA-Z246.1-13: Security management for petroleum and natural gas industry systems. It provides a performance-based approach for operators to establish governance, conduct planning, implement & improve security operations (including detection & mitigation practices) and refine the security management program through change management and audit processes.
While CSA Group is significantly involved in product certification, it does not certify security devices other than those incorporated in information technology equipment certified to IEC 1950.

**Underwriters Laboratories (UL)**

UL is an alternative to CSA established in 1894. It is an independent non-profit organisation that writes standards, tests products for safety and certifies them.\(^{618}\)

ULC Standards writes the standards for security and alarm equipment, systems and services, and it also administers the ISO TC 21 and IEC TC 79 committees for Canada.

**Canadian General Standards Board (CGSB)**

CGSB is a federal government organisation that offers standards development and CA services in support of the economic, regulatory, procurement, health, safety and environmental interests of stakeholders (government, industry and consumers).\(^{619}\) Since 1979, CGSB has delivered independent certification and qualification programmes where products are assessed against performance and quality standards.

CGSB offers standards for security personal and training programmes but no standards for security products and services.\(^{620}\) Its standards include:

- CAN/CGSB-133.1-2008 - Security Officers and Security Officer Supervisors - Phase I Training of Security Officers and Supervisors
- CAN/CGSB-133.1-2008 - Security Officers and Security Officer Supervisors - Phase II Suppliers of Security Officers and Supervisors

CGSB does not provide testing services or certification for any equipment.

**Canadian Procedural Documents (CAN-PS)**

Canadian Procedural Documents (CAN-PS) provide the Canadian public with the *policies, procedures and criteria of the Standards Council of Canada* for activities such as accreditation and international standardisation,\(^{621}\) specially: management systems CBs, inspection bodies, product and service CBs, calibration and testing laboratories, personnel CBs and stand-

\(^{618}\) It has developed more than 800 standards for safety, and millions of products and their components are tested to ULs safety standards. Information available on: http://www.crownaudio.com/certifmarks.htm


\(^{620}\) According to the head of UL Standards Department.

\(^{621}\) The following CAN-Ps may be outlined:
ards development organisations. National Standards of Canada adopted as CAN-PS must be developed and maintained by accredited SDOs according to the latest version of CAN-P-1.

**Canadian ISO Technical Committees (TCs)**

The following TCs provide important examples on Canada’s involvement in international security standardisation.

<table>
<thead>
<tr>
<th>ISO TC</th>
<th>Topic</th>
<th>Participation (P/-O-Member)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC/JTC 1/SC 17</td>
<td>Cards and personal identification</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 27</td>
<td>IT Security techniques</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC JTC 1/SC 31</td>
<td>Automatic identification and data capture techniques</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 37</td>
<td>Biometrics</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 68</td>
<td>Financial services</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 85</td>
<td>Nuclear energy, nuclear technologies, and radiological protection</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 92</td>
<td>Fire safety</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 223</td>
<td>Societal security</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 224</td>
<td>Service activities relating to drinking water supply systems and wastewater systems – Quality criteria of the service and performance indicators</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 247</td>
<td>Fraud countermeasures and controls</td>
<td>P</td>
</tr>
<tr>
<td>ISO/PC 284</td>
<td>Management system for quality of private security company (PSC) operations - Requirements with guidance</td>
<td>-</td>
</tr>
<tr>
<td>ISO/TC 292</td>
<td>Security</td>
<td>P</td>
</tr>
<tr>
<td><strong>Total P+O</strong></td>
<td></td>
<td><strong>11+0</strong></td>
</tr>
</tbody>
</table>

Figure 85: Canada’s involvement in selected security-related ISO TCs

**4.2.5. The Security Conformity Assessment Framework**

Three important players in the Canadian CA infrastructure are the CSA Group as well as the other three SDOs ULC, CGSB, and BNQ.

**CSA**

As shown earlier, CSA has a few security standards. In addition, it provides, for example testing & certification, product evaluation, education & training, energy efficiency verification,
functional safety, sanitation testing, EMC testing, project & lab management, quality & risk management and worker & workplace safety. \textsuperscript{622}

UL

The previous section showed UL’s standardisation activities. UL also provides testing, inspection and certification for the security and alarm industry. Equipment and systems for access control, fire, security, signalling covering safety, performance and software, services for transaction security systems and equipment conformance and also a Certificate Program for Central Monitoring Fire and Security Companies and their services are provided by UL. \textsuperscript{623}

CGSB

According to the previously discussed analysis, CGSB offers standards for security personnel and training programmes. It also provides CA services, including programmes for certification of products and services, registration of quality and environmental management systems, and related services. These services are provided in support of economic, regulatory, procurement, health, safety and environmental interests. \textsuperscript{624}

Security-related CA is also conducted in Canada’s public sector. More information is given below and in the next chapter.

Public organisations

Public organisations are important players in Canada’s security certification infrastructure. Several examples are provided below.

Transport Canada is responsible for security issues at Canada’s airports, marine, rail and road. Linked to the airport field, it also provides certification of drones. More information will be given in the next chapter. \textsuperscript{625}

In the IT field, the Government of Canada is responsible for Common Criteria certification. In Canada, a Common Criteria Evaluation and Certification Scheme (hereinafter, CCS) is a Canadian independent third party evaluation and certification service for measuring the trust-

\textsuperscript{622} CSA covers the following areas: appliances, chemicals energy efficiency, fuel burning equipment, gas accessories & components, gas appliances & equipment, hazardous locations, heating & air conditioning, home entertainment, industrial controls & switchgear, information technology (IT), lighting products, mobile homes - recreational vehicles / occupational health & safety medical - laboratory equipment, photometrics, plumbing products, process control & power supplies, telecommunication - sensing and signaling equipment, water quality, wire and cable and finally, wiring devices.

\textsuperscript{623} UL comprises the following areas: chemicals and chemical products, constructions, elastomers & protective and other coatings, electrical and electronic products, environmental testing and occupational health and safety, machinery, marketplace products - consumer and business, nondestructive examination, non-metallic minerals and products, textiles and fibrous materials and wood products.

\textsuperscript{624} CGSB provides the following themes: carpets and underlay, construction materials, medical products, office furniture, packaging, paints and coatings protective clothing, security personnel and testing services.

\textsuperscript{625} Further information about TC available at: Transport Canada TC, About Transport Canada, 27.02.2014. https://www.tc.gc.ca/eng/aboutus-menu.htm
worthiness of IT security products providing assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.\textsuperscript{626}

The IT product is identified in a certification report, and it has been evaluated and approved under the Canadian Common Criteria Evaluation and Certification Scheme (CCS). This approval carries with it a certificate (red maple leaf). Further information about common criteria of best practices is found on subchapter 4.8.4.2. of this Deliverable.

**Institutions responsible for scenario-based testing of security solutions**

Within the public sector, institutions such as the Royal Canadian Mounted Police (RCMP) and the Ministry of Public Safety and Security are responsible for scenario-based testing of security solutions. Some work is also done by ULC Inc. The Information Technology Association of Canada (ITAC), Canadian Fire Safety Association (CFSA), Canadian Fire Alarm Association (CFAA), Electrical Contractors Association of Ontario (ECAO)\textsuperscript{627} and the members of Canada also address these needs.

**Other certification organisations in Canada (in general)**

Other national organisations that certify PSS are the following: Intertek Testing Services NA Ltd., trading as Intertek, Price Water House Coopers LLP, KPMG Performance Registrar Inc, and Quasar (Quality Systems Assessment Registrar).

International certification organisations that can be found in the Canadian market include: Beijing Zhonglian Tianrun Certification Center (ZLTR), BSI Group America Inc. (also operating under BSI Inc.), DEKRA Certification B.V., DQS Medizinprodukte GmbH, International Quality Registrars Corporation, Laboratoire National de métrologie et d'Essais (LNE) - Division certification G-MED (trading as LNE/G-MED and G-MED) among others.

**4.2.6. SELECTED SECURITY CERTIFICATION BODIES AND THEIR WORK**

**CSA**

The CSA mark demonstrates that products created by public or private organisations have been tested and certified in an independent process controlled by CSA. Thus, if companies meet the demands required during the process, CSA certifies that they meet a specific standard. The process carried out by CSA is divided into two phases:


\textsuperscript{627} Source: interview by CRISP partner
**Contact with CSA**

First of all, the organisation is provided with a *reference number* that will be used on all future communications about the Project. Then, it will need to sign and return a *Product Service Agreement* that outlines the working relationship. Finally, it will be asked for the following.

A) *Product samples*: the organisation has to send its product samples to the laboratory indicated in the packet. If its sample is large, or its production run is limited, a CSA Group technical representative may need to visit its facility(s).

B) *Technical information*: it could be asked to provide additional technical information about its product. If its products were tested by another accredited organisation, it can include its test reports.

Once all of the necessary paperwork has been received by CSA Group, the technical representative assigned to the project will test the product and subsequently will be in contact with the organisation if any issue arise during the testing process.

**Certification**

Once all the requirements outlined in the standards are met, CSA Group will issue a *certification report and certificate of compliance*. The next step is to return the signed service agreement indicating that it is now licensed to use the appropriate CSA mark(s) and its product will now be listed in the CSA Group Certified Product Listings (CPL).

**UL**

UL is a global independent safety science company (see chapter 4.1.5). It’s security-related certification services in Canada are described below.

<table>
<thead>
<tr>
<th>Kinds of PSS which are tested and certified in the security field</th>
</tr>
</thead>
<tbody>
<tr>
<td>UL certifies equipment and systems for access control, fire, security, signalling covering safety, performance and software and also provides services for transaction security systems and equipment conformance and also Certificate Program for Central Monitoring Fire and Security Companies and their services.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Certification process(es) in the security area</th>
</tr>
</thead>
<tbody>
<tr>
<td>In most cases, ISO 17067 Type 4 is applied.</td>
</tr>
<tr>
<td><strong>System 4 (based on testing plus surveillance from factory or open market, or both)</strong></td>
</tr>
<tr>
<td>- Samples requested by the CB</td>
</tr>
<tr>
<td>- Determination of the relevant product characteristics by testing (ISO/IEC 17025) or assessment</td>
</tr>
<tr>
<td>- Initial auditing of the production process or quality system</td>
</tr>
<tr>
<td>- Review of the test or assessment reports</td>
</tr>
</tbody>
</table>

---

- Attestation of conformity
- Issue of a licence to use certificates or marks on the products
- Surveillance by testing or inspection of samples from the factory and auditing of the production process
- Surveillance by testing or inspection of samples from the market.

This system can both indicate the impact of the distribution channel on conformity and provide a pre-market mechanism to identify and resolve serious nonconformities. Significant duplication of effort may take place for those products whose conformity is not affected during the distribution process.

**Documents which form the basis of the testing and certification process(es)**

<table>
<thead>
<tr>
<th>Standards: ISO/IEC-17020, ISO/IEC 17025, ISO/IEC-17065 are the key ones. It also can be tested to UL list of standards in this area.</th>
</tr>
</thead>
</table>

**Laws/regulations:**

- Model National Building Code of Canada and its provincial equivalents
- Model National Fire Code of Canada and its provincial equivalents
- Regulated products under the Consumer Product SAFETY Act of Canada
- Various other regulations and Laws
- Insurance and banking industry requirements for services and for the insured
- Transport Canada

**Internal guidelines/documents:** no

**Other:** no
<table>
<thead>
<tr>
<th>Standard Code</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAN/ULC-S301-09</td>
<td>Signal Receiving Centre Burglar Alarm Systems and Operations</td>
<td>This Standard covers requirements applicable to signal receiving center facilities and protection service, satellite centers, and bridging centers. Signals received from residential, commercial and financial burglar alarm systems are monitored by signal receiving center operators who process the signals and take action as appropriate for the type of signals received.</td>
</tr>
<tr>
<td>CAN/ULC-S302-M91(R1999) Amendments 1-3</td>
<td>Standard for Installation and Classification of Burglar Alarm Systems for Financial and Commercial Premises, Safes And Vaults</td>
<td>These requirements apply to the installation of protective wiring and devices connected to burglar alarm systems on financial and commercial premises, safes and vaults including the classification of extent of protection installed at individual locations.</td>
</tr>
<tr>
<td>CAN/ULC-S302-14 (SECOND EDITION)</td>
<td>Standard for the Installation, Inspection and Testing of Intrusion Alarm Systems</td>
<td>This Standard prescribes requirements for the installation of intrusion alarm systems, classification of extent of protection; and testing and inspection of intrusion alarm systems.</td>
</tr>
<tr>
<td>CAN/ULC-S303-M91(R1999)</td>
<td>Standard for Local Burglar Alarm Units and Systems</td>
<td>These requirements cover design and construction, performance, and maintenance of local burglar alarm units and systems for use in mercantile premises, mercantile safes and vaults, and bank safes and vaults.</td>
</tr>
<tr>
<td>CAN/ULC-S304-06</td>
<td>Signal Receiving Centre And Premise Burglar Alarm Control Units</td>
<td>This Standard covers construction and performance requirements for signal receiving centre burglar alarm control units, and also associated burglar alarm control units to be installed within mercantile and banking premises and on safes and vaults for protection against burglary.</td>
</tr>
</tbody>
</table>

630 Intrusion alarm systems are categorized by security level. They are further grouped as suitable for protection of a particular class of property such as premises, safes, or vaults. The selection of security level to be applied in a particular case shall be made by the responsible authority (RA). For system trouble, service response and guard response, refer to CAN/ULC-S301, Standard for Signal Receiving Centre Burglar Alarm Systems and Operations.

631 It includes signal receiving, recording and supervisory control units intended for permanent use within a signal-receiving center.

632 These requirements serve as the basis of classification of signal receiving center burglar alarm control units and it covers complete control units are contained in CAN/ULC S301, Standard for Central and Monitoring Station Burglar Alarm Systems.
<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>ULC-306-03</td>
<td>Intrusion Detection Units</td>
<td>These requirements cover intrusion-detection units for burglary protection signalling systems to be employed in outdoor or ordinary indoor (nonhazardous) locations to automatically indicate the presence of an intruder by actuating electrical control circuits.</td>
</tr>
<tr>
<td>CAN/ULC-S310-M91 (R1999)</td>
<td>Installation and Classification of Residential Burglar Alarm Systems</td>
<td>These requirements apply to the installation of alarm protection products and devices connected to form a residential burglar alarm system. These requirements include the criteria for classifying the level of protection at an individual residence.</td>
</tr>
<tr>
<td>CAN/ULC-S316-14 First Edition</td>
<td>Standard for Performance of Video Surveillance Systems</td>
<td>This standard provides minimum acceptable performance parameters for video surveillance systems. The system stakeholder determines the video surveillance system operational requirements.</td>
</tr>
<tr>
<td>ULC-S317-96</td>
<td>Standard for Installation and Classification of Closed Circuit Video Equipment (CCVE) Systems for Institutional and Commercial Security Applications</td>
<td>These requirements apply to the installation of equipment and wiring of closed circuit surveillance cameras and associated video equipment.</td>
</tr>
<tr>
<td>ULC-S318-96</td>
<td>Standard for Power Supplies for Burglar Alarm Systems</td>
<td>These requirements cover power supplies for use as components in burglar alarm systems.</td>
</tr>
</tbody>
</table>

The purpose of this Standard is to provide guidance to ensure that security video system functions and performance are achieved, to assist end users, integrators, consultants and authorities with a means to objectively define, verify, and maintain compliance to performance standards. This Standard is structured:

- To accommodate a broad range of applications;
- To reflect widely used current and emerging technologies;
- To avoid specific technological requirements that may restrict the application of advanced innovative solutions and new technology; and
- Is based on a Risk – Application method. Application of the Standard requires the practitioner to determine associated risk level based on a risk assessment of each area to be covered and determination of the primary objective for each camera associated with that area. The results may then be used to select the system class requirements for each area within the system. A set of specific functional parameters required for compliance is provided for each class or category.
<table>
<thead>
<tr>
<th>CAN/ULC-S319-05</th>
<th>Electronic Access Control Systems[^634]</th>
<th>This standard defines the minimum requirements as they apply to the construction, performance and operation of such systems and/or accessory equipment as well as recommended characteristics to meet four levels of protection with Level I (lowest level-Class I equipment) to Level IV (highest-Class IV equipment).</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAN/ULC-S321-M91 Amendments 1-2</td>
<td>Standard for Burglary Resistant Vault Doors and Modular Panels</td>
<td>These requirements cover vault doors and vault modular panels (used in the construction of vault floors, walls and ceilings), for use in financial institutions, commercial, industrial and mercantile properties, and the like, and that are relied upon to protect the contents of enclosed spaces from burglary attack[^635].</td>
</tr>
<tr>
<td>CAN/ULC-S322-92 (R1998)</td>
<td>Vault Ventilators and Vault Ventilating Ports</td>
<td>These requirements cover emergency vault ventilators and vault-ventilating ports. Products covered by these requirements are intended for installation in vaults that are used for the storage of valuables, and that are protected by special security measures that cannot be forced using normal rescue equipment, but require waiting for a time lock or similar device to release entrapped individuals.</td>
</tr>
</tbody>
</table>
| ULC-S324-93 Amendment 1 | Burglary Resistant Safes | These requirements cover burglary-resistant safes classified as follows:  
A. Tested on Six Sides:  
1. Residential Safe;  
2. Tool Resistant Safe - Class TL-15X6;  
3. Tool Resistant Safe - Class TL-30X6;  
4. Torch and Tool Resistant Safe - Class TRTL-15X6;  
5. Torch and Tool Resistant Safe - Class TRTL-30X6; and  
B. Tested on Side Containing the Door:  
1. Tool Resistant Safe - Class TL-15;  

[^634]: It is a system designed to grant to authorized persons entry to and/or exit from a controlled area and deny such entry and/or exit to non-authorized individuals by electrical, electronic or mechanical means. The extent of control of entry/exit may include the reporting and recording of related activity.

[^635]: Requirements for fire resistant rating of vaults and vault doors are outside the scope of this standard and should be determined in accordance with chapter 2 of the Supplement to the National Building Code of Canada or in accordance with ULC/ORD-C72A, Fire Resistance of Prefabricated Structure Supported Vaults. These requirements are intended to establish the burglary resistant rating of vault doors and modular panels according to the length of time they withstand attack by common mechanical tools, electrical tools, cutting torches, or any combination of these means in the hands of experienced operators. These requirements do not cover attacks with the burning bar (thermal lance) or explosives.
2. Tool Resistant Safe - Class TL-30;  
3. Torch and Tool Resistant Safe - Class TRTL-15; and  

| ULC-S327-98 | Burglar Resistant Combination Locks | These requirements cover combination locks designed for attachment on doors of safes, chests, vaults, and the like, to provide a means of locking the boltwork against unauthorized opening testing the ability of combination locks to resist unauthorized opening of the lock by manipulation methods such as sense or sight, touch, hearing or manipulation by electro-mechanical devices. |
| ULC-S328-98 | Burglary Resistant Key Locks | These requirements cover mechanical key locks categorized as follows: a cabinet locking cylinder; door locks; locking cylinders; security container key locks utilizing Type 1 and Type 2 locks; and two-key locks. |
| ULC-S330-93 | Burglary-Resistant Night Depositories | These requirements cover the construction and security performance of equipment intended to permit the deposit of cash, cheques, etc., into a security container, and to provide protection against unauthorized removal of deposits. These requirements cover: a) Products intended for permanent connection to 600V or lower potential branch circuits, and b) Products intended for cord connection to 300 V or lower potential branch circuits. |
| ULC-S332-1993(R1998) | Standard For Burglary Resistant Glazing Material | These requirements cover clear or translucent glazing material intended for indoor use, outdoor use, or indoor/outdoor use as a substitute for, or in combination with plate glass show window panels intended to resist burglary attacks of the hit-and-run type. |
| ULC-S334-98 | Burglary Resistant Electronic Combination Locks | These requirements cover burglary resistant electronic combination locks designed for attachment on doors of safes, chests, vaults, automated banking machines, depository units, and the like, to provide a means of locking the boltwork against unauthorized opening. These requirements are intended to test the ability of burglary resistant electronic combination locks to resist unauthorized opening for a limited period of time. Electronic combination locks covered by these requirements may or may not have integral protection against entry by force.\(^{636}\) |

\(^{636}\) The requirements of this Standard do not apply to components and systems external to the burglary resistant electronic combination lock which are required for the administration and operation of the locking system.
| **ULC-S337-98** | **Delayed-Action Timelocks** | These requirements cover delayed-action timelocks intended for attachment on the doors of chests, and the like, to provide a means for delaying unlocking for a predetermined length of time as protection against robbery. |
| **CAN/ULC-S338-98** | **Automobile Theft Deterrent Equipment and Systems: Electronic Immobilization** | These requirements cover electrical or electronic immobilization systems which are installed on passenger cars and light duty trucks with 12 v electrical systems. Both OEM systems and non-OEM systems shall meet the requirements of this Standard. |
| **CAN/ULC-S524-14** | **Standard for Installation of Fire Alarm Systems** | This Standard describes the requirements for the design and installation of a fire alarm system with or without voice communication capability, as defined in Section 3, Glossary. This Standard is intended to apply to both required and voluntary fire alarm installations. The requirements in this Standard address the installation for various types of fire alarm system equipment and devices. These requirements are intended to apply when the equipment and devices are required by the fire alarm system design. |
| **CAN-ULC-S525-07-EN** | **Audible Signal Devices for Fire Alarm Systems, Including Accessories** | These requirements cover electrically operated bells, sirens, horns, and similar audible signal devices, rated at 300 V or less, for fire-protective signalling service and intended for indoor and/or outdoor installation in accordance with CSA C22.1, Canadian Electrical Code, Part I, Safety Standard for Electrical Installations; and with CAN/ULC-S524, Installation of Fire Alarm Systems. Refer to CAN/ULC-S541, Speakers for Fire Alarm Systems, Including Accessories, for requirements pertaining to speakers. This standard also covers protective covers and accessories used with audible signals for fire alarm systems. |
| **CAN-ULC-S526-07-EN** | **Visible Signal Devices for Fire Alarm Systems, Including Accessories** | This Standard covers requirements for visible signal devices for use in accordance with CAN/ULC-S524, Installation of Fire Alarm Systems, and in accordance with CSA C22.1, Canadian Electrical Code, Part I, Safety Standard for Electrical Installations. This standard also covers protective covers and accessories used with visible signals for fire alarm systems. |

---

\[637\] This Standard recognizes that a fire alarm system may have additional features or functions differing from those detailed in these requirements, if the features or functions enhance the life safety of the occupants of the building; and/or the protection of the building or property. Refer to Appendix A (Informative) Explanatory Materials, Clause A1.1.
<table>
<thead>
<tr>
<th>Standardbrasstechnolename</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAN/ULC-S527-11</td>
<td>Control Units for Fire Alarm Systems</td>
</tr>
<tr>
<td>CAN/ULC-S528-14 THIRD EDITION</td>
<td>Standard for manual stations for fire alarm systems, including accessories</td>
</tr>
<tr>
<td>ULC-S529-09</td>
<td>Smoke Detectors for Fire Alarm Systems</td>
</tr>
<tr>
<td>CAN/ULC-S530-M91</td>
<td>Standard for Heat Actuated Fire Detectors for Fire Alarm Systems</td>
</tr>
</tbody>
</table>

This edition of the standard was updated to address technological advancements.
<table>
<thead>
<tr>
<th>Standard Code</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAN/ULC-S531-14</td>
<td>Standard for Smoke-Alarms</td>
<td>These requirements cover electrically operated single and multiple station smoke alarms intended for open area protection in indoor locations, in accordance with Installation of Smoke Alarms, CAN/ULC-S553; National Building Code of Canada; and National Fire Code of Canada. This standard evaluates single station smoke alarms (e.g. ionization-type, photoelectric-type, smoke alarm with supplementary heat detection type, combination smoke type, multi-criteria type), as defined by these requirements, is a self-contained fire alarm device that consists of an assembly of electrical components including a smoke sensor / chamber, alarm sounding appliance, and provision for connection to a power supply source, either by splice leads, terminals, a cord and plug arrangement or containing integral batteries to detect one or more products of combustion. These requirements, where applicable, also cover all remote accessories that are to be connected.</td>
</tr>
<tr>
<td>CAN/ULC-S533-08</td>
<td>Egress Door Securing And Releasing Devices</td>
<td>This Standard shall apply to egress door securing and releasing devices to perform the function of holding a door in the closed position and releasing the door to permit free egress when operated. Egress door securing and releasing devices are considered ancillary devices and are not an integral part of the fire alarm system.</td>
</tr>
<tr>
<td>CAN/ULC-S536-13</td>
<td>Standard for Inspection and Testing of Fire Alarm Systems</td>
<td>This Standard prescribes requirements for the inspection and testing of fire alarm systems and specifies the devices and functions to be inspected, tested, and documented for the periodic inspection and test.</td>
</tr>
<tr>
<td>CAN/ULC-S537-13</td>
<td>Standards for Verification of Fire Alarm Systems</td>
<td>This Standard prescribes inspection and test procedures for the purpose of verifying that the fire alarm system is installed in conformance with the design and CAN/ULC-S524, Standard for Installation of Fire Alarm Systems, and performs all of its intended functions as designed. This Standard is intended to apply to both required and voluntary fire alarm installations.</td>
</tr>
<tr>
<td>CAN/ULC-S540-13-EN</td>
<td>Standards for Residential Fire and Life Safety Warning Systems: Installation, Inspection, Testing and Maintenance[^639]</td>
<td>This Standard sets forth the minimum requirements for the design, installation, inspection, testing and maintenance of residential fire warning systems for use within dwelling units and care occupancies not requiring fire alarm systems conforming to CAN/ULC-S524, Installation of Fire Alarm Systems. (See Appendix A, Explanatory Materials, Clause A1.1). The installation of fire detection and alarm devices not covered by the requirements in this Standard shall be in accordance with good engineering practice and the manufacturer’s published installation instructions.</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CAN-ULC-S541-07-EN</td>
<td>Speakers for Fire Alarm Systems, Including Accessories</td>
<td>These requirements apply to speakers, rated at 300 V or less, for fire-protective signalling service and intended for indoor and/or outdoor installation in accordance with CSA C22.1 Canadian Electrical Code, Part I, Safety Standard for Electrical Installations; and CAN/ULC S524, Installation of Fire Alarm Systems. Refer to CAN/ULC-S525, Audible Signal Devices for Fire Alarm Systems, Including Accessories, for requirements pertaining to audible signal devices. This Standard also covers protective covers and other accessories used with speakers for fire alarm systems.</td>
</tr>
<tr>
<td>ULC-S545-02</td>
<td>Residential Fire Warning Alarm Systems Control Units</td>
<td>It covers requirements for residential fire warning system control units and accessories intended to be installed in accordance with the Standard for the Installation of Residential Fire Warning Systems, CAN/ULC-S540.</td>
</tr>
<tr>
<td>CAN/ULC-S552-14</td>
<td>Standard for inspection, testing and maintenance of smoke alarms</td>
<td>This Standard applies to the inspection, testing and maintenance of smoke alarms within dwelling units as well as within sleeping rooms / areas that are not part of dwelling units. (Refer to Appendix A, Explanatory Materials, Clause A1.1 and Appendix B, Enhancement of Fire Safety in Residential Occupancies.) Requirements for the installation of smoke alarms are referenced in CAN/ULC-S553, Standard for the Installation of Smoke Alarms.</td>
</tr>
</tbody>
</table>

[^639]: This Standard is intended to apply to both required and voluntary residential fire warning system installations. (See Appendix A, Explanatory Materials, Clause A1.1-Note) and it specifies how such residential fire warning systems shall be installed to perform their intended function. (See Appendix A, Explanatory Material, Clause A1.2.)
<table>
<thead>
<tr>
<th>Standard Code</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAN/ULC-S553-14</td>
<td>Standard for installation of smoke alarms</td>
<td>This Standard applies to the installation of smoke alarms within dwelling units as well as within sleeping rooms / areas that are not part of dwelling units. (Refer to Appendix A, Explanatory Material, Clause A1.1 and Appendix B, Enhancement of Fire Safety in Residential Occupancies.) Requirements for the inspection, testing and maintenance of smoke alarms are referenced in CAN/ULC-S552, Standard for Inspection, Testing and Maintenance of Smoke Alarms.</td>
</tr>
</tbody>
</table>
| CAN/ULC-S559-13 | Equipment For Fire Signal Receiving Centres And Systems | This Standard covers requirements for fire signal receiving centre and systems which include transmitting, receiving equipment and proprietary fire signal receiving centre equipment and control unit accessories for use in accordance with the following:  
- CAN/ULC-S524, Installation of Fire Alarm Systems;  
- CAN/ULC-S561, Installation and Services for Fire Signal Receiving Centres and Systems;  
- Figure 1A, Typical Arrangement of Equipment for Fire Signal Receiving Centres and Systems; and  
- Figure 1B, Recommended Demarcation between Fire Alarm Control Unit and Signal Transmitting Unit at the Protected Premises. |
| CAN/ULC-S561-13-EN | Standard for Installation And Services For Fire Signal Receiving Centres And Systems | This Standard covers the:  
- Construction, operation, installation, inspection and tests applicable to fire signal receiving centres for fire protective signalling services utilizing fire signal receiving centre facilities and satellite centres and bridging centres;  
- Construction and operation of a proprietary fire signal receiving centre; and  
Installation, inspection and tests applicable to fire signal transmitting unit and its field device inputs at the protected premises. |

---

640 It includes protected premise unit and receiver for ordinary (non-hazardous) indoor and outdoor locations. Programming methods, test, service and other software intended for use with the equipment for fire signal receiving centres and systems and signal receiving units used in fire signal receiving centres, satellite centres, signal processing centres and bridging centres are covered by the requirements in the Standard.
<table>
<thead>
<tr>
<th>CAN/ULC-S572-10</th>
<th>Standard for photoluminescent and self-luminous exit signs and path marking systems</th>
<th>This Standard covers requirements for photoluminescent and self-luminous exit signs and path marking systems and the requirements for photoluminescent and self-luminous exit signs and egress (exit) path marking systems intended for installation as required by applicable codes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAN/ULC-S576-14</td>
<td>Standard for Mass Notification System Equipment and Accessories</td>
<td>These requirements cover discrete electrical control units, communication units, transport products which manipulate the data packets, interfaces, and accessories for mass notification systems. The products covered by this standard are intended to be used in combination with other appliances and devices to form an emergency communication and/or mass notification system. These requirements address emergency service personnel communication system interfaces used in the performance of their duties if that communication equipment is used to interface with or control the Emergency Communication Systems/Mass Notification Systems (ECS/MNS).</td>
</tr>
<tr>
<td>ULC/ORD-C529A-13</td>
<td>Video Image Smoke Detection System Devices</td>
<td>The Video Image Smoke Detection Systems Devices addressed by ULC/ORD-C529A-13 are to be investigated with the intent to detect the image of smoke from a fire in the field of view area defined by the limits of the camera. Installation/operating document(s) and/or product marking information provided with the product must describe the specific operating parameters of the product. This ORD utilizes the existing applicable &quot;in Canada&quot; requirements in ULC-S529, Smoke Detectors for Fire Alarm Systems, and incorporates additional requirements necessary for the evaluation of video image smoke detection system devices. Special consideration must be given to the video image smoke detection system devices regarding the overall system’s sensitivity and special care taken to reduce the possibility of false alarms.</td>
</tr>
<tr>
<td>ULC Subject C1023-1974</td>
<td>Burglar Alarm System Units, Household</td>
<td>These requirements cover household burglar alarm system units intended for use in residences.</td>
</tr>
</tbody>
</table>
Quality seal
UL uses a registered certification mark. Examples are shown below:

Certification Mark (Design):

Underwriters'Laboratories of Canada Listed
ULC & Design

Key evaluation criteria and requirements for obtaining a certificate

<table>
<thead>
<tr>
<th>product/technology/system/service: Burglar Alarm</th>
<th>evaluation criterion</th>
<th>minimum requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>apply the standard</td>
<td></td>
<td>must meet the standard</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>product/technology/system/service: Access Control System</th>
<th>evaluation criterion</th>
<th>minimum requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>apply the standard</td>
<td></td>
<td>must meet the standard</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>product/technology/system/service: Service Provider</th>
<th>evaluation criterion</th>
<th>minimum requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>apply the standard and carry out inspection</td>
<td></td>
<td>must meet the standard and pass the audits</td>
</tr>
</tbody>
</table>

Cooperation with external test laboratories in the security field
UL is not award of test laboratories in the security field

Involvement of the organisation in security standardisation
yes

Number of certificates issued in the security field annually
Unable to answer

(Mutual recognition) agreements with other EU countries/CABs in the security field
No answer

Solutions for suppliers of certified security solutions from other countries that wish to receive a certificate that is valid in Canada
No answer

UL’s certification process also includes several follow-up services.\(^{641}\)

a) Testing to maintain competency.\(^{642}\)


\(^{642}\) Competency is determined through annual assessments for the test methods and product categories covered by the Total Certification Program.
b) Follow-Up Services. A Total Certification Program (hereinafter, TCP) participant is to immediately notify the UL TCP contact engineer when a participant becomes aware of any instances, in which the Follow-Up Service prerequisite requirements have not been maintained or any other situation that may result in Follow-Up Service actions.

c) Quality management system. Total Certification Program participants have an on-going quality control programme at their engineering/testing facility. In addition, they must comply with certain responsibilities.\(^{643}\)

d) Product submittal package. As part of the Total Certification Program process, programme participants will prepare a product submittal package utilising the Product Submittal Package Form.\(^{644}\)

e) Notice of authorisation prior to applying the UL certification Mark to a product.

f) Oversight and audits every year when testing laboratory shall be reassessed under the Client Test Data.

g) Agreements. Each participant must sign and return the Client Test Data Program Agreement that covers all of a participant’s test facilities for the Client Test Data Program and Total Certification Program.

**UL markings**

UL can certify products against U.S., as well as Canadian security standards. Its markings include “cUL” or “cULus” or the enhanced mark with the ISO 3166 codes “US CA” or “CA”. Just for the U.S. either “UL” or the enhanced mark “CA plus the enhanced mark” is used. In every case, the Canadian and U.S. markings consist of four required elements:

- UL in a circle symbol that shows the name of the organisation (UL)
- Word "LISTED" in capital letters located below the name.
- Product identity or company name/file number (i.e. e314398)
- Serial or control number (i.e. 34GD).

UL shows that organisations have demonstrated the ability to manufacture and continue to manufacture in compliance with UL’s requirements with regard to one or more of the following: a specific risk (i.e. casualty, fire, etc.), performance under specific conditions, compliance

---

\(^{643}\) The responsibilities are: 1. A participant shall designate a client TCP signatory who is responsible for all aspects of the TCP. 2. A TCP signatory must demonstrate to the UL TCP contact engineer that they have sufficient training, experience and knowledge of the appropriate UL Standards and certification requirements and procedures to examine, test, document and implement design control measures for products submitted to UL under the TCP. 3. Any changes to the status of TCP personnel must be brought to the attention of the UL TCP contact engineer immediately. 4. A TCP participant is to maintain up-to-date copies of standards, directories, and other publications and materials needed to examine, test, document and implement design control of products to the applicable requirements. The UL TCP contact engineer will review these materials during each quarterly engineering oversight assessment. 5. TCP participants must conduct investigations of products for conformance with applicable requirements and establish conformance prior to using the UL Mark.

with regulatory codes, compliance with specific standards such as international standards or other condition.

Apart from the above mentioned differences between the U.S. and Canadian markings, if an organisation is interested in selling a product in the U.S., Canada and Europe, a combined UL mark for Europe, Canada and United States can be obtained. This mark may only be applied while a product remains in compliance with all certification programmes represented by the combined version of the mark.

This mark consists of the different elements: SAFETY attribute instead of LISTED and the ISO country code of CA for Canada, EU for Europe and U.S. for the United States.

**CGSB**

Canadian General Standards Board (CGSB) certification is based on the following all-inclusive process:

1. *Demonstration by suppliers.* Their products must meet the requirements of the referenced standards and are sufficiently in control to ensure they will continue to be made to these standards.

2. *Programme list:* certification programme list (CPL) or a Qualification Program List (QPL)\(^645\) describes the products and suppliers of the programme.

3. *On-going programme:* CGSB ensures the product continues conformance to the standard. This is carried out through a procedure divided into four phases: Application, Quality System Assessment, Listing/Licensing and On-going Product Testing and Facility Assessments.

**Intertek**

Intertek provides testing, inspection, certification, auditing and technical training to Canadian and international organisations. Regarding cyber security systems, it stays on top of the latest virus definitions. Its security testing solutions scan and filter for malware and viruses protect user data. If there is a specific threat or vulnerability the organisations are trying to avoid, it works with the involved organisations to define their needs and customise the testing approach that is right for them. Intertek also offers Alarm Service & Monitoring Company Certification based on the following Reference UL Standards:

- UL 681 – Installation and Classification of Burglar and Holdup-Alarm Systems
- UL 827 – Central Station Alarm Services
- UL 1023 – Household Burglar-Alarm System Units
- UL 1076 – Proprietary Burglar-Alarm Units and Systems
- UL 1641 – Installation and Classification of Residential Burglar-Alarm Systems
- UL 1981 – Central Station Automation Systems

\(^645\) These lists are available to purchasing professionals at all levels of government, corporate and institutional users, retailers, and the public.
Transport Canada

In general, security at Canadian airports is a responsibility of Transport Canada. However, it is shared among departments and agencies that work closely with Transport Canada, including the Royal Canadian Mounted Police (RCMP), Canada Border Service Agency (CBSA), the Canadian Air Transportation Security Agency (CATSA), Canadian Security Intelligence Service (CSIS), and local authorities at individual airports.

To ensure a secure aviation system, Transport Canada created the National Civil Aviation Security Program (NCASP) a programme that sets out legislation, policies, programmes, and regulations. To achieve the above has required close collaboration between its many partners (other federal departments, industry and stakeholders) to ensure the highest security aviation system, through the right balance between security, efficiency and fiscal responsibility. Regarding security aviation systems, civil and commercial aviation must be considered.

Civil aviation transport

Transport Canada is the lead for aviation security in Canada and is responsible for the development of aviation security legislation, policies, programs and regulations to prevent unlawful interference with civil aviation, as well as oversight to ensure compliance with regulatory requirements since strengthening and improving security screening of all kinds is one of its major priorities.

In this way, TC has the exclusive national competence in aviation security. It grants of clearances to persons who meet the standards set out in its Program, “Transportation Security Clearance Program” in order to prevent unlawful acts of interference with civil aviation.

Commercial aviation transport

Currently, Transport of Canada has proposed and is developing an Accreditation Plan and Cargo Screeners Certification for the freight and cargo industries and for established train-

---


648 Internal Accreditation for Freight and Cargo applies to the following industries: a specific company that wants to develop an internal training program for its own employees, the regulated entity would have to submit its internal training program to Transport Canada for review and approval or would issue training certificates to cargo screeners who successfully complete its training program, but would not have the authority to certify cargo screeners. Cargo screeners would have to apply directly to Transport Canada for their certification.

External Accreditation for Established Training Institution and Contractors would apply to: contractors and to established training institutions who wish to provide training on a commercial basis to companies that handle secure air cargo. Established training institutions would also be eligible to certify contractors, contractors and training institutions would not have the authority to certify cargo screeners. Transport Canada must approve training materials before accreditation. Contractors and training institutions would be subject to Transport Canada Oversight and Compliance Framework.
ing institutions or contractors who want to deliver an air cargo security-training programme. Henceforth, employees who wish to screen air cargo will have to be certified by Transport Canada once they complete the training.

Drones

According to the Canadian Aeronautics Act, unmanned air vehicles (UAV) are considered to be an "aircraft". An UAV system is a set of configurable elements consisting of an unmanned aircraft, its associated control station(s), the required command and control links and any other elements as may be required, at any point during flight operation.

UAV is the only term that currently has a legal basis in the Canadian Aviation Regulations that have regulated them as an aircrafts of any size that may be remotely controlled or may have an automated flight capability and are designed to fly without a human operator on board and operated by a pilot controlling them remotely. If they exceed 35 Kg in weight, they are legally considered UAVs and the operator of the model aircraft must apply for, and receive, a Special Flight Operations Certificate.

Transport Canada is responsible for establishing, managing, and developing safety and security standards regarding to UAVs which are limited by law because they are subject to licensing approvals and safety parameters set by Transport Canada. Subsequently, there are not established standards and certification schemes to set requirements for pilot licensing, certification, maintenance, or command and control of UAVs.

At present, one instrument governs UAVs, the Special Flight Operating Certificate (SFOC). The Standard 623.65(d) Special Flight Operations outlines the requirements for complying with the Regulations Respecting Unmanned Air Vehicle.

---

649 Cargo Screeners Certification: In addition to completing the required training, cargo screeners would be required to be certified by Transport Canada. Both internal and external accredited training programmes would issue training certificates to cargo screeners who successfully complete their training programmes. Transport Canada will then individually certify cargo screeners to make them legally authorized to screen air cargo. http://www.tc.gc.ca/eng/aviationsecurity/asc-training-accreditation-236.html


652 Model Aeronautics Association of Canada (MAAC) and Academy of Model Aeronautics (AMA) Members Application Process. Section 12 of the Staff Instructor. http://www.tc.gc.ca/eng/civilaviation/standards/general-recavi-uav-4161.html#toc12_0

653 Flying an unmanned aircraft? You may need permission from Transport Canada http://www.tc.gc.ca/media/documents/ca-standards/Infographic_Permission_to_fly_a_UAV_Print_English.pdf

654 Canadian Aviation Regulations. Sub-part 603, Divisions I, II, III and IV. Standard 623.65(d): (1) The following standards apply to the application for and the operation of an unmanned aeroplane, rotorcraft or airship pursuant to CAR 602.41. (2) An application for a Special Flight Operations Certificate for the purpose of conducting the flight of an unmanned aircraft other than an unmanned free balloon or a model aircraft shall be received by the appropriate Regional Transport Canada General Aviation Office, at least 20 working days prior to the date of the proposed operation or by a date mutually agreed upon between the applicant and Transport Canada. (3) The following constitutes an application for a Special Flight Operations Certificate for the purpose of operations in paragraph (1) above: (a) the name, address, and where applicable, the telephone number and facsimile number of the applicant; (b) the name, address, and where applicable the telephone number and facsimile number of the person designated by the applicant to have operational control over the operation (Operation Manager); (c) method by which the Operation Manager may be contacted directly during operation; (d) the type and purpose of the operation; (e) the dates, alternate dates and times of the proposed operation; (f) a complete description, including all pertinent flight data on
According to Transport Canada policy, a SFOC must be issued for each operation pursuant to section 5.1 in the Transport Canada Staff Instruction (SI) 523.001 regarding “The Review and Processing of an Application for a Special Flight Operations Certificate for the Operation of an Unmanned Air Vehicle (UAV) System.”

Safe flight is Transport Canada’s primary concern when issuing the SFOC and privacy considerations are notably absent in the licensing requirements or regulations established by Transport Canada. At present, there are approximately 300 individually licensed UAV operators in Canada. An applicant is granted a short-term authority or an authority that is site-specific, noting its operations have been conducted in a safe way in a previous process.

4.2.7. SUMMARY AND CONCLUSION

The Canadian framework for standards is tightly-regulated, systematic, effective, efficient, sustainable and flexible, ensuring market functionality. The Standards Council of Canada (SCC) is established by regulation as a crown corporation and controls the entire accreditation process. The organisation reports to the Parliament through the Minister of Industry and oversee Canada’s National Standards System. It prescribes policies and procedures for developing NSC and coordinates Canada's stakeholder’s participation in the accreditation and standardisation system. The four Standards Development Organisations (SDO), ULD, CSA, BNQ and CGSB, apart from being considered as SDOs, are the main CBs in their fields of specialisation. They are highly skilled, experienced and well-known for creating strong and consistent standards that are nationally and internationally recognised. These certification organisations have their own good practices which generate increased reliance on the Canadian market for authorities, manufacturers and consumers.

Despite the EU Regulation 765/2008 requiring the establishment of one national accreditation body (NAB) per country and the replacement of systems with different involved organisations, making Canada’s structure incompatible with Europe’s, there are still possibilities for

---


Transport Canada suggests that once an initial SFOC has been issued, the subsequent SFOC applications should be able to be expedited. While Transport Canada will initially require a full SFOC application for each use, after a number of successful operations Transport Canada may issue a SFOC for a longer period of time so long as Transport Canada receives an informal notice (which can be given by email) at least two days before each specific operation. A Regional Transport Canada General Aviation Office will restrict the geographic area of a SFOC it issues to the area which it administers. The Canadian Bar Association, Sarah Fitzpatrick & Kenneth Burnett, “Regulation and use of drones in Canada”, no date. http://www.cba.org/CBA/sections_airandspace/newsletters2013/drones.aspx
learning from the Canadian structure, for example UL’s position in the market for security solutions and examples for standards and certification schemes for alarm and CCTV systems.

4.2.8. REFERENCES


Canadian Unmanned Aircraft System Regulations, ICAO RPAS Symposium, Karen Tarr, Transport Canada, 24 March 2015


Flying an unmanned aircraft? You may need permission from Transport Canada http://www.tc.gc.ca/media/documents/ca-standards/Infographic_Permission_to_fly_a_UAV_Print_English.pdf


Model Aeronautics Association of Canada (MAAC) and Academy of Model Aeronautics (AMA) Members Application Process. Section 12 of the Staff Instructor. http://www.tc.gc.ca/eng/civilaviation/standards/general-recavi-uav-4161.html#toc12_0


https://www.scc.ca/en/accreditation

The Canadian Bar Association, Sarah Fitzpatrick & Kenneth Burnett, “Regulation and use of drones in Canada”, no date.

Transport Canada TC, About Transport Canada, 27.02.2014.
https://www.tc.gc.ca/eng/aboutus-menu.htm

UL, “Follow-Up Services”, 2015.
http://ul.com/offerings/global-field-services/follow-up-services/

UL, Technical Guidance Documents.

4.3. **BRAZIL**

4.3.1. **INTRODUCTION**

Brazil, the fifth largest country regarding its territory and population is also the sixth largest economy worldwide and its landscape of security PSS has a number of interesting characteristics. This study builds on interviews with representatives from Brazil’s regulatory and standardisation body ANAC, with experts from several units of its accreditation body INMETRO, market surveys, data base searches and additional sources from different CBs.

4.3.2. **SHORT DESCRIPTION OF THE COUNTRY’S SECURITY INDUSTRY**

The Brazilian security market is experiencing an above average growth. A study from AHP International\(^657\) shows that the growth percentages has varied between 15% and 20% since 2005 to reach a value of R$ 24 bn, the equivalent of € 9.4 bn in the year 2013. The U.S. Department of Commerce even estimates the market value of 2013 to be US$ 24 bn (21.6 bn).\(^658\) The expectations and forecasts regard this trend as continuing, at least for the next couple of years. As an example, the U.S. professional association ‘Security Industry Association’ expects a tripling of the electronic security market between 2012 and 2017 (from US$ 592 million (€ 476 million) to US $1.8 bn (€ 1.6 bn) by 2017).\(^659\) According to their study, the current market breaks down as follows: ‘video surveillance (39.6 %), access control (20.8 %), intrusion alarms (19.2 %), fire detection and suppression (10.4 %), and electronic article surveillance (10 %)’. Financial institutions are the market’s main end-users, spending approximately US$1 bn per year in security equipment and services.\(^660\)

In particular there are three reasons for the growth of the Brazilian market for security solutions and the expectations for further growth.\(^661\) The first one is the new increase in breaking-in, car thefts, threats and other criminal activities; the second one includes the worldwide known sport events of 2014, the football world cup and the Olympic Games in 2016. As a last reason, only 9 % of all the security equipment is bought by private households (numbers of 2012). A rise of the demand by private households is expected.

The giant wave of criminal activity causes a feeling of insecurity and encourages people to protect themselves. Brazil has a long history with violence, gangs, drug lords and murder, but implemented measures for the reduction of such crime. In contrast to these positive developments, low level crimes are regarded as an important problem. For example, there have been several raids on restaurants as well as shopping malls. An additional newer problem is caused


by organised burglaries targeting apartments in city parts, which are not covered by security measures or whose security systems are too old. Furthermore, unsupervised supermarket parking lots have become the hunting grounds for car thefts. Not only cars are disappearing but also numerous trucks.\textsuperscript{662}

In response, most restaurants have begun installing cameras and hiring private security guards, similarly with the shopping malls. Starting in 2013, all new cars have to be equipped with a tracking device. Furthermore, parking lots are being monitored with surveillance cameras and security personnel.\textsuperscript{663}

In summary, the combination of several issues led to the expectation of a continuous growth in demand for both security cameras and private security protection:

- the steady increase in burglaries,
- the wealthier middle-class,
- new apartments and hotels, which have yet to invest in security and protection as well as
- the fact that until now most security equipment was not bought by private households.\textsuperscript{664}

In addition, the sports events have increased the demand for security coming from the state. This demand especially includes surveillance equipment, identification infrastructure and protected data processing. To ensure a high level of security, the government established secretary position inside the Ministry of Interior.

To prepare for the soccer games, specific command and control centers to merge, process and use data from the civil police, the military police, private security firms, firefighters and emergency services as well as an additional central communication center in Brasilia and a backup center in Rio de Janeiro were established. This caused specific demand for data processing equipment and technology.

Another requirement was related to the number of security personnel. The Ministry set up the goal of having one security person for 30 spectators, which resulted in substantial demand for schooling and training.\textsuperscript{665}

Finally the Ministry wished to increase the surveillance in both the cities and in the airports. Stadiums and their surroundings, the main streets of the game locations, bus stations and the airports were to be protected by camera surveillance, which led to a massive boom in the demand for surveillance equipment. In addition, Brazil plans to equip all public buses with access control technology and CCTV systems.\textsuperscript{666}

Another effect linked to the sports event was the competition of the hotels and training grounds to hosts the sports teams. Most hotels invested enormous sums to increase their security, both in surveillance equipment and personnel, to be selected.

\textsuperscript{662} Döhne, op. cit., 2012
\textsuperscript{663} Döhne, op. cit., 2012
\textsuperscript{664} von Delhaes-Guenther, op. cit., 2013.
\textsuperscript{665} von Delhaes-Guenther, op. cit., 2013.
\textsuperscript{666} von Delhaes-Guenther, op. cit., 2013.
Important Brazilian providers of security solutions include GRABER – Soluções Integradas, G4S, VIP Security, Surcom Internacional Importação e Exportação, Sectra, Montrel SMH Sistemas, Sanlia Tecnologia, Secur, Meta Telecom Comercial, Securiton, Spark Controles, Semaseg. Nevertheless Brazil still has a high import rate, with 56% of the security equipment being imported. The U.S. represents Brazil’s main exporter of security solutions, followed by Israel, Japan, Canada, Germany and the UK. The study of AHP International brings forward the argument that Brazil’s own production is lacking in quality compared to products from abroad. If the prices are similar, clients rely more on the foreign products for better quality.

4.3.3. THE SECURITY STANDARDISATION FRAMEWORK

4.3.3.1. INTRODUCTION

As described in CRISP’s Deliverable 2.1, conformity assessment systems (CAS) consists of three sections: the voluntary sector, the law regulated sector and the sovereignty sector. The nature of such a national system also influences the standards framework presented in this specific country. Brazil considers security mainly as an issue of the government and the military, not as a subject of open standardisation. Therefore the ‘sovereignty sector’ has a much broader scope than in Europe.

The security related duties are divided as follows:

- Brazil’s national standardisation organisation Associação Brasileira de Normas Técnicas (ABNT) is responsible for civil security including construction, fire hazards, infrastructure (buildings) and IT security.
- National security including protection against terrorism and organised crime, airport security, border control and guns is under the responsibility of the government.
- Security against explosives is even an issue of the military.

In addition, there are, for example, strict laws related to guns and explosives.

To illustrate the interrelation of the two security areas, The FIFA World Cup 2014 and the Olympic Games 2016, which will be held in Rio de Janeiro, have had no influence on security standardisation because they are an issue of the government. Nevertheless, Brazil has event management standards, which also address civil security issues, as well as standards for the safety of the ground.

Besides its membership at ISO and IEC, ABNT participates in the two regional standards cooperations AMN and COPANT. AMN stands for MERCOSUR Standardization Association and its key participants are Brazil, Argentina, Paraguay, Uruguay and Venezuela.

---

COPANT is the Pan American Standards Commission and has members from all countries in the region. Both organisations do not develop own standards. AMN aims to define common needs and to present them at ISO. COPANT has the same principle but a broader scope.

Like their member ABNT, both institutions are mainly responsible for safety issues, not for security. Nevertheless they provide interesting aspects to learn from. Aldaz-Carroll, reporting on standards and CA procedures in the MERCOSUR countries Argentina, Brazil, Chile, Peru and Uruguay, has examined a range of approaches for upgrading standards and conformity procedures in these countries. The case study, whilst not focused on security, is a useful example of how regional approaches have been utilized in order to upgrade standards and provide better standards systems.

Aldaz-Carroll concludes that where there is a need to upgrade standards and CA procedures, regional approaches and harmonization processes to better standards allied with regional trade agreements have yielded promising results. Citing the problems of upgrading standards unilaterally, Aldaz-Carroll argues that coordinated efforts to upgrade standards are essential to ensure partners’ standards and CA requirements. In his case study, he notes that in order to minimise an array of problems, many countries have upgraded their standards following a coordinated harmonisation process with other trading partners. Pursuing a ‘coordinated path’, through one of two distinct coordinated approaches is a means of ensuring that issues are kept to a minimum: the cooperation approach, followed by bilateral trade agreements and by multilateral cooperative agreements and the regional trade agreement approach, followed by members of an regional trade agreements and involving not only upgrading standards, but also the regional harmonisation of standards.

### 4.3.3.2. Specific Security Standards

This chapter gives an overview of Brazilian standards in the three security fields ‘Security of the Citizens’, ‘Security of infrastructures and utilities’ and ‘Border Security’. It provides information on relevant standards and specific ABNT committees.

#### Security of the Citizens

<table>
<thead>
<tr>
<th>Area</th>
<th>Duties and documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection against organised crime, terrorism</td>
<td>Government accountability</td>
</tr>
<tr>
<td>Explosives</td>
<td>Responsibility of the military (Exército - Army) no civil standards</td>
</tr>
</tbody>
</table>

---


Fire Hazards

TC ABNT/CB-03 is responsible, in particular for the following standards:

- ABNT NBR IEC 60695-2-12:2013 Fire hazard testing Part 2-12: Glowing/hotwire based test methods - Glow-wire flammability index (GWFI) test method for materials
- ABNT NBR IEC 60695-10-2:2008 Fire hazard testing Part 10-2: Abnormal heart - Ball pressure test
- ABNT NBR IEC 60695-2-10:2006 Fire hazard testing Part 2-10: Glowing/hotwire test methods - Glow-wire apparatus and common test procedure

Security of infrastructures and utilities

<table>
<thead>
<tr>
<th>Area</th>
<th>Duties and documents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Building design</strong></td>
<td>TC ABNT/CB-02 is entrusted with this issue and also responsible for the following standards:</td>
</tr>
<tr>
<td></td>
<td>- ABNT NBR 7678:1983 Segurança na execução de obras e serviços de construçao</td>
</tr>
<tr>
<td><strong>Energy/transport communication grids</strong></td>
<td>responsibility of ABNT/CB-03 Electrotechnical ABNT/CB-16 Transportation and Traffic and ABNT/CEE-116 Energy Management</td>
</tr>
<tr>
<td><strong>Surveillance</strong></td>
<td>no standards exist</td>
</tr>
<tr>
<td><strong>Supply chains</strong></td>
<td>three standards of ABNT/CEE-97 Gestão de Segurança para Cadeia Logistica exist:</td>
</tr>
<tr>
<td></td>
<td>- ABNT NBR ISO 28004-1:2013 Security management systems for the supply chain - Guidelines for the implementation of ABNT NBR ISO 28000 Part 1: General principles</td>
</tr>
<tr>
<td></td>
<td>- ABNT NBR ISO 28001:2011 Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance</td>
</tr>
<tr>
<td></td>
<td>- ABNT NBR ISO 28000:2009 Specification for security management systems for the supply chain</td>
</tr>
</tbody>
</table>
Border Security

The Brazilian government is responsible for the certification of all security solutions. In general, Brazil adopts ISO/IEC standards. There are almost no national security standards instead of ISO/IEC standards, but there are national regulations, which are used as alternatives.

National security-related standards in addition to international ISO/IEC/ITU standards exist only in the field of building design. Examples are provided by ABNT NBR 8681:2003 Versão Corrigida:2004 Actions and safety of structures – Procedure and ABNT NBR 7678:1983 Segurança na execução de obras e serviços de construção.

Specific interrelations between standardisation, regulation and certification exist in the field of fire hazard and fire fight control. For example, companies have to follow Fire Hazard Regulations to get a certificate. In many cases these regulations include mandatory national standards. Another example is provided by a Regulation on general requirements for basic safety and essential performance. Regarding certification, an expert describes the Brazilian approach as follows:

‘In Brazil there is a very strong regulation particularly in the area of fire safety. The Brazilian standards are used and cited in the procedures for certification and subsequently regulators require these products to be sold after the acquisition of the certificates.’

More information on this topic is given in chapter 4.3.4.

4.3.3.3. International activities in the security field

Brazil is an active member of ISO and IEC. Its involvement in international security-related standards committees is shown in Figure 8685 and will be explained in detail.

<table>
<thead>
<tr>
<th>ISO TC</th>
<th>Topic</th>
<th>Participation (P-/ O-Member)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC/JTC 1/SC 17</td>
<td>Cards and personal identification</td>
<td>-</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 27</td>
<td>IT Security techniques</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC JTC 1/SC 31</td>
<td>Automatic identification and data capture techniques</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 37</td>
<td>Biometrics</td>
<td>-</td>
</tr>
<tr>
<td>ISO/TC 85</td>
<td>Nuclear energy, nuclear technologies, and radiological protection</td>
<td>O</td>
</tr>
<tr>
<td>ISO/TC 92</td>
<td>Fire safety</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 223</td>
<td>Societal security</td>
<td>P</td>
</tr>
</tbody>
</table>
Brazil participates for example in ISO/TC 223 via ABNT and adopts the standards of this committee. It is also involved in international standardisation activities in the field of information security. But there are also specific pre-requisites, which result in Brazil’s absence in several other security-related ISO TCs. ISO 284 Management systems of private security companies provides an example for that. Brazil is not involved in this TC because security companies are regulated by the Brazilian government. In addition, there are strict regulations regarding the use of fire arms. Furthermore, Brazil will not participate in the new ISO TC 292 Security because all topics covered by the TC fall under the responsibility of Brazil’s government. In contrast, ABNT is involved in all ISO activities in the safety field.

### 4.3.4. ***THE SECURITY CONFORMITY ASSESSMENT FRAMEWORK***

The foundation of Brazil’s CA framework is SBAC, the Brazilian System of Conformity Assessment, which is coordinated by INMETRO, which is a government organisation, which is responsible for safety and several security issues, health, environment and prevention of deceptive practices. The member of the International Accreditation Forum (IAF) is also active at ISO CASCO, IEC CAB as well as in several ISO TCs in the fields of safety and risk.

#### Structure

Among other departments within its structure, INMETRO consists of the Diretoria de Avaliacao da Conformidade and the unit Coordenaceao-general de Acreditatcao.

The Diretoria de Avaliacao da Conformidade (Dconf) is responsible for technical regulations (TR) and certification schemes for 3rd party certification including the development of CA schemes, leading to INMETRO’s scheme ownership in numerous areas. While TRs define prerequisites, the conformity assessment schemes specify the assessment procedure.

---

672 Security in this context also refers to items such as toys and helmet.

673 CASCO and CAB are independent of specific subjects
Coordenacao-geral de Acreditacao (CGCRE) is responsible for the accreditation of CABs and governmental organisations. Its tasks include laboratory accreditation, inspection body accreditation and CB accreditation. Based on these duties, it has three units for the three specific accreditation services. At governmental level, INMETRO accredited:

- the Agência Nacional de Aviação Civil (ANAC) which is responsible for aviation
- the Agência Nacional de Telecomunicações (ANATEL), the national telecommunication agency
- the Agência Nacional de Vigilância Sanitária (ANVISA), the Brazilian health surveillance agency and
- the Ministério da Agricultura, Pecuária e Abastecimento (MAPA), which is responsible for agricultural issues.

All these organisations issue Technical Regulations (TRs) which specify certification requirements. The importance of the deliverables from these organisations and those of ABNT is different and while Brasilian TRs are mandatory, standards are volunatry.

**Certification schemes**

In general, the foundation of Brazil’s certification schemes are ISO schemes (not only in the security field). If available, ISO, IEC and ITU standards are used as a foundation of TR and adopted as ABNT standards. Such standards can only be quoted in technical regulations if they are translated into Portuguese, which means that they are published as an ABNT standard. If no international standard exist, INMETRO uses home-grown ABNT standards. Relevant fundamental standards are those from ISO CASCO like ISO 17000-series on CA as well as ISO 17067 for certification.
Figure 8887 gives an overview of technical regulations, CA schemes and the organisations which are responsible for the conformity assessment in Brazil. As described earlier, many security fields are under the control of the State. To give an example, the Agência Nacional de Aviação Civil (ANAC) created technical regulations for airport security and INMETRO created the relevant certification scheme.

<table>
<thead>
<tr>
<th>Field of conformity assessment</th>
<th>Technical Regulation</th>
<th>Conformity Assessment Schemes</th>
<th>Conformity Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire Hazards</td>
<td>Defence Ministry</td>
<td>Defence Ministry and Federal Police</td>
<td>Defence Ministry and Federal Police</td>
</tr>
<tr>
<td>Security-related prerequisites for roads, airports and ports in general</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Border security, surveillance of ports, airport, frontiers</td>
<td>Defence Ministry, Federal Police, Federal Revenue (Receita Federal), which belongs to the Ministry of Finance. INMETRO has a partnership with Federal Revenue, but is for example not responsible for the schemes for security scanners at airports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Airports paths for take-off and landing</td>
<td>INMETRO in collaboration with department of roads</td>
<td>INMETRO in collaboration with department of roads</td>
<td>department of roads</td>
</tr>
<tr>
<td>Air area at airports (areas behind inspection)</td>
<td>INMETRO + ANAC</td>
<td>INMETRO</td>
<td>ANAC</td>
</tr>
<tr>
<td>Trucks with dangerous cargo</td>
<td>INMETRO</td>
<td>INMETRO</td>
<td>div. inspection bodies which are accredited by INMETRO</td>
</tr>
<tr>
<td>Helmets</td>
<td>INMETRO</td>
<td>INMETRO</td>
<td>Federal Revenue</td>
</tr>
<tr>
<td>Hazards in the field of agriculture</td>
<td></td>
<td>MAPA (Ministry of Agriculture)</td>
<td></td>
</tr>
<tr>
<td>Hazards in the field of food</td>
<td></td>
<td>ANVISA</td>
<td></td>
</tr>
<tr>
<td>Hazards in the field of Explosives</td>
<td></td>
<td>Defence Ministry</td>
<td></td>
</tr>
</tbody>
</table>

Abbreviations: ANAC = Agência Nacional de Aviação Civil, ANVISA = Agência Nacional de Vigilância Sanitária, MAPA = Ministério da Agricultura, Pecuária e Abastecimento

Source: Own figure based on a draft of an INMETRO expert
Figure 88: Organisations and duties in the Brazilian conformity assessment system

Important certifiers related to safety issues include ABNT which is one of the main certifiers in Brazil, BSI, TÜV Rheinland, SCS, Falkenbauer and BNT.

As mentioned earlier, security is mainly an issue of the state. Therefore, there are only a few security fields, in which private bodies offer security-related certification, e.g. the information security (and electric fences in the future).
Information security

Certification bodies, which work based on ISO/IEC 17021 Conformity assessment - Requirements for bodies providing audit and certification of management systems are accredited by INMETRO. The CA scheme for Information Security includes

- IEC standards for IT
- ISO/IEC 27001 - Information security management
- no regulation because the certification is voluntary.

INMETRO’s website\(^674\) shows the CBs, which are accredited in this area. The list includes for example in the field of ‘Sistemas de Gestão em Tecnologia da Informação – OTI’ (Management Information Technology Systems) the organisation FCAV - Fundação Carlos Alberto Vanzolini but no specific information could be found for ‘Sistemas de Gestão de Segurança da Informação – OTS’ (Safety Management Information Systems).

A specific issue is the certification in the field of cryptography. The foundation of Brazil’s relevant certification activities is ISO/IEC 27001 - Information security management, but the certification process is subject of the Ministry of Science and Technology.

Electric fences

The field is regulated by INMETRO and the future certification scheme has three parts:

- NBR IEC 60335-2-76 Household and similar electrical appliances - Particular requirements for electric fence energizers
- Portaria 371 / 2009
- ISO IEC 17065 Conformity assessment -- Requirements for bodies certifying products, processes and services

Related certification services will be offered soon.

In addition, there are security fields, which are not a subject of certification but of inspection. In the field of dangerous goods, for example, INMETRO has accredited numerous inspection bodies.

Additional searches in the INMETRO database\(^675\) together with experts from INMETRO plus a follow-up statement by an INMETRO expert unveiled that INMETRO accredited no additional private CBs or security certification schemes in the security field.

\(^674\) Link to the results: http://www.inmetro.gov.br/organismos(resultado_consulta.asp,

\(^675\) Search words included, for example, the Portuguese terms for alarm systems, CCTV systems and biometrics.
4.3.5. **SELECTED SECURITY CERTIFICATION BODIES AND THEIR WORK**

### 4.3.5.1. PUBLIC SECTOR

This section refers in particular to ANAC and its duties regarding the security of Airport Infrastructure. ANAC is the Agência Nacional de Aviação Civil. Additional information is provided on the Department of Airspace Control (DECEA).

**ANAC**

The National Agency of Civil Aviation (ANAC), founded in 2006, is the Brazilian aviation authority. This agency is responsible for the regulation of matters of safety and security concerning civil aviation. Based on ANAC’s establishment in 2006 the responsibility for national civil aviation issues was outsourced from the Brazilian airforce. As a special Federal autarchy with the status of a regulatory agency, ANAC is linked to the Civil Aviation Secretary of the Presidency of Brazil.\(^{676}\)

The Department of Airport Infrastructure (Superintendência de Infraestrutura Aeroportuária – SIA) has responsibilities related to aerodromes concerning planning, **safety, security and airport inspection**. Among other duties, its **Engineering Division** is responsible for the establishment of **standards and rules for airport design** and master plans. In addition, it keeps Brazilian aerodromes database updated.

The **Operations Division** is responsible for the establishment of safety standards, rules, guidelines and inspections related to aerodromes operations, maintenance, emergency response and safety management systems (SMS). It is also responsible for conducting airport operational certification process. Activities also comprise, for example, analyses of operational safety at airports during construction, aerodrome manuals and plans and certification of firefighting training centers.

The most important division in the security context is the **Facilitation and Security Division** (Gerência de Faciliação do Transporte Aéreo e Segurança da Aviação Civil Contra Atos de Interferência Ilícita – GFSI). Its duties include the establishment of technical guidelines, standards and rules for all aspects related to air transport facilitation and security against unlawful acts. This division is also responsible for regulating airlines, airport and cargo operators, airport services, besides aviation security training centers.

In addition, there is the **Regulations, Standards and Systems Division** (Gerência de Normas, Padrões e Sistemas – GNPS), which is responsible for planning, coordination and support of activities related to studies, proposition of normative acts projects or issuance of opinion on matters for the Airport Infrastructure office, including quality control of normative acts proposed. Identification, management, standardisation, audit, improvement and communication of the work processes within the office as well as creation of systems to support management.

\(^{676}\) National Civil Aviation Agency Brazil, “About ANAC”, no date. http://www2.anac.gov.br/ingles/aboutanac.asp
Other units include the Privatized Airports Branch (Gerência Técnica de Coordenação de Concessões – GTCC), the Airport Fiscalization Division (Gerência de Fiscalização Aeroportuária – GFIS) and the Urban Relations and Environment Section (Divisão de Relações Urbanas e Meio Ambiente - DRUM) which develops studies, analysis and technical guidelines concerning the regulation of aircraft noise and wildlife hazard at airports.

According to an expert, ANAC’s development of regulations for airport security builds on material from the American Federal Aviation Administration (FAA). As mentioned in chapter 4.3.4, ANAC is accredited by INMETRO. A close relationship between both organisations exists and INMETRO coordinates ANAC’s certification activities. The duties are divided as follows: ANAC develops regulations, INMETRO creates related certification schemes and ANAC uses these schemes for certification.

**Department of Airspace Control (DECEA)**

The Department of Airspace Control (DECEA) is subordinated to the Brazilian Ministry of Defense and to the Airforce. DECEA is responsible for the strategic and systematic control of security and fluency of the Brazilian airspace as well as its defense. In the following, a specific focus is put on DECEA’s certification of UAVs (unmanned aerial vehicles).

Guidelines for licensing and operating UAVs are currently being revised in the context of Law Project No. 16/2015 and are likely to be put under stronger control of DECEA. The proposal suggests the following aspects to be relevant for licensing: incorporation in the National Defense Strategy; infringement of the right to privacy of citizens and property; research and scientific development; purpose of use for public safety operations; professional fitness of operator to fly UAVs.

Currently relevant documents related to UAV certification include:

- An untitled ANAC document from 1999 applies to the use of model drones and defines, among others, the areas of use and flying altitudes.
- Published by ANAC, Regulamento Braileiro da Aviação Civil (RBAC) 21, the Brazilian Civil Aviation Regulation specifies regulation of aeronautic products.

---


678 National Civil Aviation Agency Brazil, “RPAS – Sistemas De Aeronaves Remotamente Pilotadas”, no date. 
http://www.2.anac.gov.br/rpas/

http://www.decea.gov.br/autorizacoes-para-voos-de-vant-entenda-melhor/


681 ANAC, Regulamento Braileiro da Aviação Civil, RBAC n21 Emenda n01, 2011. 
D2.2: Consolidated report on security standards and certification

- Supplement IS 21-002, Revision A, titled "Emissão de Certificado de Autorização de Voo Experimental para Veículos Aéreos Não Tripulados“ (Certification of Authorisation of experimental flights for UAVs) specifies the issuing of Experimental Flight Authorization Certificates (CAVE) for research, development and educational purposes.

For the experimental use of RPAs (Remotely-Piloted Aircrafts) a CAVE complying with section 21.191 und 21.193 of RBAC 21 has to be acquired.

Currently there are no specific regulations for the commercial use of UAV. Still, general guidelines of RBHA 91 (general rules for civil aviation), RBAC 21 (s.a.), RBAC 45 (identifiers) and RBAC 47 (registration of aircrafts) apply.

Besides ANAC and DECEA, the Brazilian Organization for the Development of Aeronautical Certification (DCA-BR) is an important player in Brazil’s security certification infrastructure. It is a non-profit organisation that is highly involved in the certifications and regulatory processes, for example by providing consulting services.

**4.3.5.2. Private Conformity Assessment Bodies**

As shown earlier, INMETRO’s database lists no CB, which has a national Brazilian accreditation to offer security-related certification. A few additional foreign CABs are mentioned by Standards.org.

Besides Bureau Veritas Brazil and Nippon Kaiji Kyokai (ClassNK) Brazil, which for example certifies ships based on the International Ship and Port Facility Security (ISPS) Code, the database provides information on Cotecna Brazil. Cotecna Brazil belongs to the Swiss-based Cotecna group. It provides, for example, non-intrusive inspection (X-ray imaging as well as explosive and radiation detection). Cotecna’s website specifies the objects of these inspections: Inspection of goods at point of origin and at points of transit as well as Non-intrusive inspection of containers and cargo. The CA services build, for example, on C-TPAT, ISO 28000, the Business Alliance for Secure Commerce (BASC) and Authorized Economic Operator (AEO).

---

683 The website http://www.standards.org/certification_bodies/ was visited several times in summer 2014. However it has been closed down in 2015 and is no longer available.
685 ClassNK, Home, no date. http://www.classnk.or.jp
4.3.6. **SUMMARY AND CONCLUSION**

Brazil provides an interesting case study that delivers a contrasting perspective on security solutions as it differs from Europe in that many aspects of security-related CA are managed by the state or government organisations. Therefore the SDO ABNT as well as the regional standards cooperations AMN and COPANT, are only partly involved in security standardisation. Furthermore, Brazil participates in security-related committees at ISO and IEC, but opts to employ national solutions developed by governmental organisations to handle specific security issues in its society involved in the relevant ISO TC. Contrastingly, activities at CEN and CENELEC, the security standardisation Mandate M/487, projects like CRISP and many other examples demonstrate Europe’s innovative approach in this regard to identify specific synergies and to handle security issues together.

Nevertheless, Brazil’s interesting methodology for the certification of drones, a type of certification not existing in most countries, may serve as a valuable reference for CRISP’s WP 4 that deals with certification schemes in selected security fields including drones. The case study from Aldaz-Carroll also highlights that it is not only necessary to develop certification infrastructures, but also to implement mechanisms which allow an appropriate upgrading by the countries involved.

4.3.7. **REFERENCES**


---

German Trade & Invest, 2012
http://www.gtai.de/GTAI/Navigation/DE/Trade/markte,did=602734.html

Latin America Geospatial Portal, “Project establishes operating rules for UAV in Brazil“, 25.02.2015.

National Civil Aviation Agency Brazil, “About ANAC”, no date.
http://www2.anac.gov.br/ingles/aboutanac.asp

National Civil Aviation Agency Brazil, “RPAS – Sistemas De Aeronaves Remotamente Pilotadas”, no date.
http://www2.anac.gov.br/rpas/

SIA, “SIA report predicts Brazilian security market will triple within five years” 2012.
http://www.gsnmagazine.com/article/26918/sia_report_predicts_brazilian_security_market_will


4.4. **INDIA**

4.4.1. **INTRODUCTION**

This chapter provides a case study of the Indian security industry, specifically with regard to standardisation and certification of security PSS. Aims are as follows:

- Provide an overview of the Indian Security Market
- Provide an overview of current Indian security standards
- Identify and analyse the scopes, concepts and procedures and bodies responsible for/administering the schemes.

Through desk research, best practice standards and certification schemes were identified and these are presented here. Due to the complexity of the Indian standardisation and certification landscape and the number of entities involved it was a difficult task to focus specifically on security PSS as these fall under different policy categories and responsibility for these are divided between many different ministries and organisations. Currently, the Indian government has a strong focus on cyber security and data protection and this emphasis is presented in this report.

4.4.2. **SHORT DESCRIPTION OF INDIA’S SECURITY INDUSTRY**

Since the Mumbai terrorist attack in 2008 the Indian government has been steadily increasing homeland security and raising awareness in the country for higher protection. As a result India’s homeland security spend is now larger than the defense budget of many countries.690

The budgetary allocation for the Ministry of Home Affairs (MHA) for the year 2013-14 was just under US$ 11 bn and is expected to near the US$ 20 bn mark by 2017-18. Of course only a part of that contributes to the overall HS market in India. Nevertheless, according to estimates the Indian internal security industry is also slated to be worth at least US$ 20 bn by 2018 with the central government accounting for a third of this spend.691

trAIDe analysis692 (2012) of the Indian security market, reveals that it consists mostly of electronic products and that majority of security equipment is imported from Germany, US, UK and Japan. Most in demand are integrated systems and software (23% of the market), CCTV (22%), smoke detectors (18%) and metal detectors (14%).

Forecasts expect continuing growth, both in the security as well as the safety aspects of the market and some have predicted steady positive growth in the double digit range, (up to +21% per year until year 2016).693

---

691 Jha, op. cit., 29 July 2014
693 trAIDe, op. cit., 2012
Further to providing an analysis of the full security market, the trAIDe report also gave an overview of each market segment:

- **Close Circuit Television (CCTV)**
  The main final clients for CCTV, which make up nearly 50% of all buyers, are shops, enterprises and hotels. The most sought out qualities in this market are price and the technological capabilities. Current trends are to equip industry areas with surveillance cameras, and research and development sites. Further future investments will come with investments in big infrastructure projects like airports, ports or logistics centers. Regulation from the Reserve Bank of India (RBI) requires all banks to have CCTV and other security systems installed. Also, the Indian government has had the underground equipped with CCTV to increase both security and public awareness.

- **Metal Detectors**
  In this segment, about 25 Indian and international players are active. A third of the market segment is composite of local manufacturers or through imports from Taiwan and China. The typical distribution structure is characterized by direct sales to end users or system integrators. The vast majority of bought metal detectors in 2012, namely 85%, have a high sensitivity, meaning they are intended to find weapons, especially knives. Those same 85% were bought by: the industry, without reasons given; while the commercial sector, hotels and companies explain their choice in the strong threat of terrorism and a need for security. The Government is also a large scale investor in metal detectors for their buildings, since the 2008 Mumbai attack.

- **Firefighting & Smoke Detectors**
  This market is mainly an import market, with Germany having around 26% of the total import value. There is no visible trend in the market as there have not been big changes from one year to another. There exist security regulations for firefighting and smoke detectors. They differentiate different types of buildings and have various degree of required compliance. The requirements are set by the construction companies which afterwards also carry the responsibility in case of malfunctioning. Certification is offered by the BSI India but costs may vary. CE and UL certified products are also recognized and accepted. This sector experienced a boom, closely related to the trend of building big shopping malls, which require high quality firefighting systems and smoke detectors. At the same time, awareness has risen among the population so private investors have been increasing their investment in this field.

- **Biometrics**
  This market is dominated by fingerprints recognition products, which make up to 93% of the entire market. The two main clients are institutions (38%) and the Indian government (35%). The government has recently been investing in big projects which require biometric products, such as the possibility of introduction E-passports. Iris Scans are still mainly underdeveloped but companies are pushing the development further and investing in the products.
RFID (Radio Frequency Identification)
There is no numbers for RFID available as they belong to a bigger group of products and the following numbers concern that bigger market. There are three big investors in this market; namely infrastructure (30%), industry (22%) and health care (18%). The RFID is mainly an import market with some native players. There are high expectations for growth in this market as certain frequencies have just been opened up for RFID. Retail and the pharmaceutical sectors are also both increasing their use of RFID.

Cash in Transit (CiT)
This market is mostly operated by private CiT companies. The larger companies offer comprehensive services related to Cash Management, which exceed cash transportation only. The sub market of armored vehicles is dominated by imports from Germany.

Internal Security
The terrorist attacks of Mumbai, in the year 2008, have had a notable impact in this market. In addition, India has a giant border problem, not only with their land borders but also with their border shore and water borders. They therefore require state of the art technology and a high number of equipment for civil security.694

4.4.3. The security standardisation framework

Overall, India has made efforts to harmonize national standards with international norms and ISO standards. There are however still a number of national standards in use. The Indian standardisation system is complex and is composite of various bodies and Ministries. India’s participation in international standardisation (ISO, IEC, and ITU) is at inter-governmental level since standardisation is within the remit of government ministries.

Bureau of Indian Standards is India’s National Standardisation Body under the Department of Consumer Affairs, which is under the Ministry of Consumer Affairs, Food & Public Distribution. In addition to BIS there are a 51 organisations and government departments who develop and publish standards within their respective field.695 The standardisation framework found relevant to this report consists of the Department of Consumer Affairs. It serves as the official member and sets policy for Indian participation in the International Organization for Standardisation (ISO) and International Electro technical Commission (IEC)

BIS is comprised of representatives of industry, consumer organisations, science and research organisations, professional organisations, technical institutions, Indian government ministries, and members of parliament.

Each governmental ministry can define regulations and policies in its area of competence. Furthermore, within a ministry, several departments may be involved in standards and regula-

695 A full list of all standardisation organisations in India can be found on BIS website Standards Data, 2010-2011, http://standardsdata.in/
tions within their area of competence. For example, the Ministry of Communications and Information Technology has two departments, each of which participate in standards related activities: Department of Telecommunications (DoT), which is a member of ITU which is responsible for developing and monitoring national telecommunications standards, policies and legislation and the Department of Electronics and Information Technology (DeitY) which responsible for the electronics and IT industry and covers rest of the ICT standards; e.g. for Internet, e-governance, cyber security, national knowledge network, R&D in electronics & IT etc.

Standardisation Technical Committees are chaired by the senior officials from the concerned Departments of Union Ministry, with participation from academia, concerned trade association representatives and selected relevant private sector experts. The recommendations of such Committees form the basis for further discussions by BIS Technical Committee. The BIS TC (Standardization Technical Committee(s) output is then provided for public consultation, where support by industry representatives is taken into consideration for additional potential updates of the standard.696

This chapter will focus on presenting the key ministries, departments and organisations that make up the country’s standardisation, accreditation and certification framework and specific focus will be on security.

**Department of Consumer Affairs**

The Department of Consumer Affairs (DCA) is a department under the Ministry of Consumer Affairs, Food & Public Distribution. DCA oversees BIS as well as issues regarding trade, regulation of commodities, black market prevention, training in legal metrology, standards, eight and measures, consumer affairs and is also a national test house.

One of the roles of DCA is the formulation of Standards and the strengthening of CA of products and services. This is carried out through BIS. The current strategy of DCA is to amend the Bureau of Indian Standards Act, 1986, which has not been amended since it was passed. The aim is to bring in several innovations and improvements in the manner in which standards are formulated, popularised and enforced. The strategy in this area comprises the following elements:

- Implementation of schemes to popularise and widen the process of standardisation and providing training to various stakeholders.
- Amendment of the BIS Act for removal of restrictions imposed by reference to “Scheduled Industry”.
- Introduction of self declaration of adherence to the relevant Indian standards as an alternative mechanism to compulsory licencing.
- Introduction of Hallmarking of precious metal articles under compulsory certification regime.
- Introduction of provision for compounding of offences punishable under the Act.

- Protection of consumer rights through strict standardisation of commodities.\(^{697}\)

**Bureau of Indian Standards**

Bureau of Indian Standards is the National Standardisation Body, which was set up, on 1st April 1987, as a result of the Bureau of Indian Standards Act, which was passed by Parliament in 1986. However, national standardisation started in 1947 when the Indian Standards Institution was established, which operated until 1986. In 1952 ISI was also given responsibility for operating certification marking scheme. BIS is a member of ISO and currently participates in 655 Technical committees and 3 PDCs.

<table>
<thead>
<tr>
<th>ISO TC</th>
<th>Topic</th>
<th>Participation (P/-O-Member)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC/JTC 1/SC 17</td>
<td>Cards and personal identification</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 27</td>
<td>IT Security techniques</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC JTC 1/SC 31</td>
<td>Automatic identification and data capture techniques</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 37</td>
<td>Biometrics</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 68</td>
<td>Financial services</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 85</td>
<td>Nuclear energy, nuclear technologies, and radiological protection</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 92</td>
<td>Fire safety</td>
<td>O</td>
</tr>
<tr>
<td>ISO/TC 224</td>
<td>Service activities relating to drinking water supply systems and wastewater systems - Quality criteria of the service and performance indicators</td>
<td>P</td>
</tr>
<tr>
<td>ISO/PC 284</td>
<td>Management system for quality of private security company (PSC) operations - Requirements with guidance</td>
<td>P</td>
</tr>
<tr>
<td>Total P+O</td>
<td></td>
<td>9</td>
</tr>
</tbody>
</table>

Figure 89: India ISO TC participation for selected standards development

The Results Framework Document for BIS for 2014-2015, published by the Indian Government outlines the formal objectives and functions of BIS:

1. To formulate need based standards and participate in international standardisation.
2. To satisfy the customer’s need for quality and safety of goods and services through operation of Certification Schemes (Product Certification, Registration, Management System Certification, Hallmarking) of BIS.
3. To test samples generated through product certification scheme of BIS.

\(^{697}\) Department of Consumer Affairs, Strategic Plan 2011-2015 (Updated – 2013), no date.
http://consumeraffairs.nic.in/consumer/?q=node/472 P15
4. To organise training programmes for industry to enable & encourage them to produce quality goods.
5. To generate awareness on standards, standard mark, and safety & quality of products through seminars, awareness programmes and publicity campaigns.
6. To improve the quality and competitiveness of Indian industry and thereby enhance export of Indian goods and services through conformance to Indian standards and acceptance of BIS mark by importers.
7. To improve transparency in functioning and thereby allowing greater participation of stakeholders in various activities of BIS.

Functions of BIS are to:

1. publish and promote the Indian Standard, in relation to any article or process;
2. recognise as an Indian Standard any standard established by any other institution in India or elsewhere, in relation to any article or process;
3. specify a Standard Mark to be called the BIS Certification Mark which shall be of such design and contain such particulars as may be prescribed to represent a particular Indian Standard;
4. grant, renew, suspend or cancel a licence for the use of the Standard Mark
5. seek recognition of the Bureau and of the Indian Standards outside India on such terms and conditions as may be mutually agreed upon by the Bureau with any corresponding institution or organisation in any country.

BIS is currently involved in the following activities:

- Standards Formulation
- Certification: Product, Hallmarking and Systems
- Foreign Manufacturers Scheme
- Registration Scheme
- Testing & Calibration Services
- Sale of Indian standards and other publications
- International Activities
- I-Care Activities (for consumer and industry)
- Promotional Activities
- Training Services
- Information services
- Financial: Resources - Mobilization and utilization
- Trade Facilitation Cell
- Library Services.

BIS has formulated over 19,000 standards in various technology areas. According to policy standards formulation has been harmonised with ISO guidelines and BIS is also a signatory to the ‘Code of Good Practice for preparation, adoption and application of standards’.

---

700 Bureau of Indian Standards, About Us, no date. http://www.bis.org.in/
Standards development process in BIS is carried out through a process outlined on the BIS websites. The steps undertaken in standards development are shown in Figure 90 and Figure 9190 presents India’s standardisation activities between 2012 and 2014.

Further to formulating needs based Indian standards BIS has made the decision to harmonise national standards with international standards wherever feasible.\textsuperscript{701} This is seen to facilitate adoption of international standards by all market segments. This is evident when standards applicable to new security technologies are examined, as most of these are identical to relevant ISO/IEC security standards.

Technical Committees within BIS are responsible for the development and publication of Indian standards. The Committee structure comprises of Division Councils, Sectional Committees, Subcommittees and Panels. Sectional committees include representatives of various stakeholder groups such as consumers, regulators, government bodies, industry, scientists, technical experts, test organisations and consultants. The committee structure of BIS seeks to bring together all those with substantial interest in particular projects, so that standards are developed with national interests in mind and so that all significant viewpoints are taken into account. BIS technical committees’ decisions are made on the basis of consensus.

Standardisation work is carried out in 14 departments within BIS. As there is not one department dedicated to security a search was carried out within the documents of all departments in order to find where security standardisation work is carried out. Within most departments there is a focus on health and safety standards formulation, but as the focus is on security these were excluded from analysis. After a review of documents, it emerged that security standardisation activity was clustered within the departments of Mechanical Engineering, Electronics and Information Technology. Following are lists of committees and security standardisation activity to demonstrate the scope and to what extent Indian security standards are national and international in nature.

How Indian Standards are made

- Any Ministry of the Central Government, State Governments, Union Territory Administrations, consumer organisations, industrial units, industry-associations, professional bodies, members of the Bureau and members of its technical committees may submit proposals to the Bureau for establishing a standard or for revising, amending, or cancelling an established standard by making such request in writing.
- The work of formulation of standards on any specific subject shall be undertaken when the Division Council concerned is satisfied as a result of its own deliberations or on investigation and consultation with concerned interests that the necessity for standardisation has been established.
- When the subject has been so investigated and the need established, the Division Council concerned shall assign the task of formulating the standard to an appropriate Technical Committee or shall appoint a new Technical Committee for the purpose.
- When request for establishing a standard for any specific subject has not been accepted after its due consideration, the proposer is informed of the decision.
- A draft standard prepared and duly approved by a Committee is issued in draft form and widely circulated for a period of not less than one month amongst the various interests concerned for critical review and suggestions for improvement. The wide circulation may be waived if so decided by the Sectional Committee where the matter is urgent or non-controversial.
- Special attention is given to multidisciplinary areas such as energy conservation, environmental protection, rural development and safety.
- The appropriate Technical Committee thereafter finalises the draft standard giving due consideration to the comments that may be received. The draft standard after it has been approved by the Sectional Committee and submitted to the Chairman of the Division Council concerned for adoption on its behalf.
- All established standards are reviewed periodically, at least once in five years, to determine the need for revision or withdrawal. Standards which in the opinion of the Sectional Committee need no revision or amendment are reaffirmed by the Sectional Committee.

Figure 90: Development of Indian standards\textsuperscript{702}

\textsuperscript{702} Bureau of Indian Standards, How Indian Standards are made, no date, http://www.bis.org.in/stl/pros_setting_std.asp
Security Equipment Sectional Committee

Standardisation activities relating to ‘Security Equipment’ are carried out by the Security Equipment Sectional Committee, which as of 15<sup>th</sup> January 2014 has developed 17 standards. The committee falls under the Mechanical Engineering Department of BIS. The scope of the committee is: “Formulation of standards for safes; cash boxes; strong room doors and safe deposit locker cabinets, ventilation equipment for banks etc.” It is to note that the standards developed within this committee are all Indian Standards (IS) while the following committees that focus on more recent security technologies have opted to adopt international ISO/IEC standards. This is in line with the BIS policy to harmonise standards with international standards for the purpose of simplification and broader appeal to the market and industry.

<table>
<thead>
<tr>
<th>Standard Number</th>
<th>Standard Title</th>
<th>Reaffirmed/Printed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IS 550(PT 2): 2003</strong></td>
<td>Safes, Part 2 Tests for burglary Resistance</td>
<td>May 2013</td>
</tr>
<tr>
<td><strong>IS 550(PT 3):2005</strong></td>
<td>Safes, Part 3 Tests for fire resistance</td>
<td>February 2010</td>
</tr>
<tr>
<td>*IS 1046:1992</td>
<td>Cash Boxes - Specifications</td>
<td>February 2013</td>
</tr>
<tr>
<td>IS 7152:1992</td>
<td>Book room doors - Specifications</td>
<td>February 2013</td>
</tr>
<tr>
<td>IS 11188(PT 2):1991</td>
<td>Vault (Strong room) doors: Part 2 – Test for burglary resistance</td>
<td>December 2010</td>
</tr>
<tr>
<td>IS 11188(PT 3):1991</td>
<td>Vault (Strong room) doors: Part 3 – Test for fire resistance</td>
<td>December 2010</td>
</tr>
</tbody>
</table>

---

**IS 14203:1999**  | Fire resisting record protection cabinet - Specification  | February 2010
--- | --- | ---
**IS 14387:2005**  | Vaults – Air ventilators - Specifications  | December 2010
**IS 14505:1998**  | Fire resisting magnetic media protection cabinets - Specification  | February 2013
**IS14512:1998**  | Safe cum safe deposit lockers - Specification  | May 2013
**IS 15369:2003**  | Code of practice for construction of vault (strong room)  | May 2013

Figure 92: Indian security equipment standards

The committee has further got the following standards under print:

<table>
<thead>
<tr>
<th>Standard Number</th>
<th>Standard Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOC: ME 24 (1247)</td>
<td>Draft Indian Standard Safes Part 1 Specification (Fifth Revision)</td>
</tr>
<tr>
<td>DOC: ME 24 (1279)</td>
<td>Draft Indian Standard fire resisting (insulating) filing cabinets – specification (Second Revision)</td>
</tr>
<tr>
<td>DOC: ME 24 (1280)</td>
<td>Draft Indian Standard Cash Boxes Specification (Forth Revision)</td>
</tr>
<tr>
<td>DOC: ME 24 (1281)</td>
<td>Draft Indian Standard safe deposit locker cabinets-specification (Third Revision)</td>
</tr>
<tr>
<td>DOC: ME 24 (1283)</td>
<td>Draft Indian Standard Fire Resisting Computer Media Protection Cabinets-Specifications (First Revision)</td>
</tr>
</tbody>
</table>

Figure 93: Indian security equipment standards under print

*Information Systems Security and Biometrics Sectional Committee*

Scope: ‘To prepare Indian Standards relating to biometrics and security aspects of Information Systems & smart cards.’

---

706 Bureau of Indian Standards, op. cit., July 2014, p. 56
707 Bureau of Indian Standards, op. cit., July 2014, p. 57
<table>
<thead>
<tr>
<th>Standard Number</th>
<th>Standard Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS 14356:1996</td>
<td>Guide for protection of information resources</td>
</tr>
<tr>
<td>IS 15116:2012 / ISO/IEC 10116:2006</td>
<td>Information Technology - Security techniques - Modes of operation for an n-bit block cipher (First Revision)</td>
</tr>
</tbody>
</table>

Figure 94: System security and biometric standards in India

*Indicates Standard under revision **Indicates standard to be revised / indicates that the standard is a total adoption of the following ISO/IEC standard
The committee further has the following draft standards issued in wide circulation:

<table>
<thead>
<tr>
<th>Standard Number</th>
<th>Standard title</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOC.LITD 17(3228)/ISO/IEC 27033-3:2010</td>
<td>Information Technology - Security techniques - Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues</td>
</tr>
<tr>
<td>DOC.LITD 17(3248)/ISO/IEC 19784-3:2007</td>
<td>Information Technology - Biometric application programming interface - Part 2: Biometric archive function provider interface</td>
</tr>
<tr>
<td>DOC.LITD 17(3249)/ISO/IEC 19784-4:2011</td>
<td>Information Technology - Biometric application programming interface - Part 4: Biometric sensor function provider interface</td>
</tr>
<tr>
<td>DOC.LITD 17(3250)/ISO/IEC 19785-1:2006</td>
<td>Information Technology - Common biometric exchange formats framework Part 1: Data element -Specifications</td>
</tr>
<tr>
<td>DOC.LITD 17(3251)/ISO/IEC 19785-4:2010</td>
<td>Information Technology - Common biometric exchange formats framework Part 4 Security block format -Specifications</td>
</tr>
</tbody>
</table>

Figure 95: Draft system security and biometric standards in India

Alarms and Electronic Security Systems Committee: IEC/TC79

The scope of the committee is ‘to prepare Indian standards relating to the protection of buildings, persons, areas and properties against fraudulent action having the purpose to enter in a place or take or to use something without permission and other threat related to persons’.

The committee liaises with the IEC/TC 79 Alarm and Electronic security systems.

There is currently one draft standard in formulation: DOC. LITD 26(0) Indian Standards on Alarm and Electronic Security Systems (To be prepared).

The standards document was sent out to interested parties as well as members of working group LITD 26 and all members of the Electronics and Information Technology Division Council on 13 January 2015 for review, comment and input. The distributed document states that that the standards are identical with corresponding ISO/IEC Standards and will be adopted as Indian Standards following consultation and consensus agreement. The document contains the following standards for review and agreement.

---

711 Bureau of Indian Standards, op. cit., 15 March 2014
### Department of Electronics and Information Technology (DeitY)

The Department of Electronics and Information Technology (DeitY) deals with e-Development of India through a multi-pronged strategy with a focus on (with the last of the topics of relevance to this report):

- **e-Government:** Infrastructure creation for delivery of services
- **e-Industry:** Promotion of Electronics hardware manufacturing and IT Enabled Services
- **e-Innovation:** The provision of support of RD&I in emerging areas of technology
- **e-Education:** Development of e-Skills and Knowledge networks
- **e-Security:** Securing of India’s Cyberspace

With regard to standards, DeitY is responsible for the promotion of standardisation, testing and quality in IT and standardisation of procedure for IT applications and tasks.

One of DeitY’s divisions is dedicated to Cyber Laws and E-Security and works within the remit of the National Cyber Security Policy from 2013. The policy acknowledges that:

“Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation-states and non-state actors. Cyberattacks that target the infrastructure or underlying economic..."
wellbeing of a nation state can effectively reduce available state resources and undermine confidence in their supporting structures. A cyber related incident of national significance may take any form; an organized cyberattack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets."\(^{713}\)

The policy’s key aim is to ‘build a secure and resilient cyberspace for citizens, businesses and government; and one of the objectives is to ‘create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people)’.\(^{714}\) The policy furthermore sets out a strategy for creating an assurance framework which promotes the adoption, CA and certification of compliance to global best practice in cyber security. The strategy also aims to build an infrastructure for the above, using standards and guidelines, for example: ISO 27001 ISMS certification, information security system audits, Penetration testing/Vulnerability assessment, application security testing and web security testing. The policy also interestingly focuses on the use of Open Standards to better facilitate interoperability and data exchange among different products or services and the enhancement of the availability of tested and certified IT products based on open standards.

**Quality Council of India**

The Quality Council of India (QCI) is registered as a non-profit society and was set up by the Government of India and three industry associations\(^ {715}\) to establish and operate a national accreditation structure for India. The Council plays an important role in propagating, adoption of and adherence to quality standards in education, healthcare, environment protection, social sectors, governance and other areas in India. The key objectives of QCI are to:

- Establish and maintain an accreditation structure in the country;
- Provide right and unbiased information on quality related standards;
- Spread quality movement in the country through National Quality Campaign;
- Facilitate the upgrade of equipment and techniques related to quality;
- Represent India’s interest in International forums;
- Help establish brand equity of Indian products and services.\(^ {716}\)

QCI oversees accreditation through four National Accreditation Boards: for Certification Bodies (NABCB), for Education and Training (NABET), for Hospitals and Healthcare Providers and Testing and Calibration Laboratories (NABL). For the purpose of this report we will only focus on a short profile of the NABCB as the other boards lie outside its remit.


\(^{714}\) DeitY, op. cit., 2013.

\(^{715}\) Associated Chambers of Commerce and Industry of India (ASSOCHAM), Confederation of Indian Industry (CII) and Federation of Indian Chambers of Commerce and Industry (FICCI)

\(^{716}\) Quality Council of India, Driving Quality for National Well Being, no date. http://www.qcin.org/about.php
National Accreditation Board for Certification Bodies (NABC"

The NABC provides accreditation to Certification and Inspection Bodies in accordance with international standards (e.g., ISO/IEC 17011 Conformity assessment -- General requirements for accreditation bodies accrediting CABs) and other relevant international/national standards and guidelines. NABC works on a national and international level and represents the interests of Indian industry as a member of International Accreditation Forum (IAF) and the Pacific Accreditation Cooperation (PAC).

The database on the website of the NABC lists 129 Certification Bodies working within India. NABC currently offers the following accreditation programmes:

- Environmental Management Systems
- Energy Management Systems
- Food Safety Management Systems
- Inspection Bodies
- Information Security Management Systems
- Information Technology Service Management Systems
- Occupational Health and Safety Management Systems
- Product Certification Bodies
- Quality Management Systems

Whilst some CBs are local, many international CBs also have offices within India e.g., TUV, BSI and SGS. As security is not a distinct category on the NABC website, nor is there a way to filter search according to narrower categories, it is difficult to ascertain within which programmes certification takes place (aside from Information Security Management Systems). In the following chapter, the focus will be on building short profiles of the largest certification schemes and the most prominent Indian CBs to demonstrate certification processes, standards and schemes.

4.4.4. SELECTED SECURITY CERTIFICATION BODIES AND THEIR WORK

The research project Seconded European Standardization Expert (SESEI) in India presents the following figure to outline the CA, testing & certification landscape in India.

This Chapter will focus on two CBs, Bureau of Indian Standards and STQC both of which provide overall certification services nationally. Furthermore, a profile of the Data Security Council of India will be presented as it is in the process of building privacy and security assessment frameworks in ICT.
Bureau of Indian Standards (BIS)

BIS operates one of the largest certification schemes in the world, ISI Mark, with over 26,500 licensees, which cover over 900 products. The scheme allows a licensee to use the ISI mark on their product. BIS also operates a Foreign Manufacturers Certification Scheme which allows international manufacturers to use the ISI Standards Mark. Over 350 licenses have been granted in 40 countries around the world.\(^\text{718}\)


\(^{718}\) Bureau of Indian Standards, Testing - Overview, no date. http://www.bis.org.in/lab/lab_overview.asp
For granting a licence to a manufacturer BIS evaluates whether required infrastructure is in place and assesses the capability of the manufacturer to produce and test the product according to the relevant Indian Standard. BIS takes production samples which are tested in BIS laboratories or recognised independent laboratories to ensure conformance. The ISI scheme is voluntary in nature aside for 92 product standards which have been made mandatory by the Indian Government for purposes of ensuring health and safety of consumers. The BIS certification scheme does not clearly present security product or system certification and the following information has thus a general focus on BIS certification activities.

### Testing

BIS operates eight test laboratories, which support BIS product certification activities and especially the ISI mark scheme as products certified under the scheme are tested at said laboratories. To ensure that BIS laboratories are up to date according to international developments within the field of testing, they are accredited by the National Accreditation Board for Calibration and Testing Laboratories (NABL) according to the IS/ISO/IEC 17025 standard. Due to heavy workload at the BIS laboratories, BIS operates the Laboratory Recognition Scheme (LRS) which recognises outside laboratories and test certificates and there are 147 BIS labs throughout India, including both government and private sector laboratories.

---


720 Government of India, op. cit., no date.
Product Certification

The BIS Product Certification Scheme provides third-party guarantee of quality, safety and reliability of certified products. The ISI certification mark (also known as Standard Mark\textsuperscript{721}) demonstrates assurance of conformity to the specification, which is ensured by “regular surveillance of the licensee's performance by surprise inspections and testing of samples, drawn both from the market and factory.”\textsuperscript{722} Manufacturers are permitted to self-certify the licenced products after ascertaining their conformity to relevant standards.

The scheme itself is voluntary in nature, and is largely based on ISO Guide 28 which provides general rules for third party certification system for determining conformity of product quality with standards. The Indian Government, however, on the grounds of public health and safety, security, infrastructure requirements and mass consumption does enforce mandatory certification on various products. This is enforced through orders, which are issued under various legislative acts. While BIS grants licences on application, the enforcement of compulsory certification is carried out by the notified authorities.

BIS has the following relevant product certification schemes:

Domestic Manufacturers Certification Scheme

Two procedures are available to applicants for certification under this scheme:

Normal Procedure – whereby the applicant is required to submit an application, for the BIS Certification Marks Licence, along with required documents and requisite fee to the nearest BIS branch office. Once an application has been approved a preliminary inspection is carried out whereby the “firm's manufacturing capability and controls, quality control techniques, facilities available and the technical skills of the personnel are evaluated. Samples of products are tested and also drawn for testing in BIS or other recognized laboratories.”

Licence to use the Standard Mark on a product is granted after BIS has ensured that the manufacturer is capable of manufacturing the product continuously in accordance with the relevant Indian Standard, especially with respect to raw materials, process of manufacture, manufacturing capability and quality control facilities including testing equipment and supervisory staff. Samples are tested in the factory, in order to bring out any deficiencies in test equipment/testing procedures and testing personnel as well as for spot establishment of quality of product. Simultaneously, samples are also drawn for testing in the independent laboratories for assessing conformity to the relevant standard. The manufacturer is required to agree to operate a well-defined Scheme of Testing and Inspection (STI) as approved by BIS from time to time, which inter alia prescribes the specific tests and the frequency for conducting them. In order to meet the expenditure incurred by BIS in operating the licence, the manufacturer also has to agree to pay a marking fee fixed by BIS for the product. Licence is granted only after the manufacturer agrees to these conditions and if the factory inspection and test reports are satisfactory.

\textsuperscript{721} “Standard Mark” means the Bureau of Indian Standards Certification Mark specified by the Bureau to represent a particular Indian Standard and also includes any Indian Standards Institution Certification Mark specified by the Indian Standards Institution" The Bureau of Indian Standards Act, 1986, Chapter One, Article 2(t). http://www.bis.org.in/bs/bsisact.htm

Initially, the license is valid for one year and can then be renewed for further period of one/two years. This is subject to satisfactory operation of license as observed by BIS during periodic inspections of factory and independent testing of samples, drawn from both the factory and the market.

**Simplified Procedure** – whereby the applicant submits samples for testing at BIS approved laboratories and submits test reports along with an application. If the test reports and other documents are deemed satisfactory, a verification visit is carried out by BIS and the license is granted thereafter if everything is found to be satisfactory. The simplified procedure is only available for products which are covered under voluntary certification.

**Foreign Manufacturers Certification Scheme**

In this scheme, a license to use the Certification Mark of the Bureau of Indian Standards, called the Standard Mark, can be granted by BIS for any product against an Indian Standard, which is amenable to certification. The Foreign Manufacturers Certification Scheme has been in operation since 2000. In this scheme, a license to use the Standard Mark, can be granted by BIS for any product against an Indian Standard, which is amenable to certification. To qualify for a licence the applicant must satisfy the following conditions:

a) Complete manufacturing facilities for the product are available in-house in the applicant’s factory at the address indicated in the application form (else, details of alternate arrangements made are to be provided);

b) Complete testing facilities for the product in accordance with the relevant Indian Standard are available in-house in the applicant’s factory at the address indicated in the application form (else, details of alternate arrangements made are provided);

c) Competent testing personnel are permanently employed, who understand the requirements of the relevant Indian Standards and are competent to carry out tests for various characteristics as per the test methods prescribed in the relevant Indian Standards;

d) The product conforms to the relevant Indian Standard (assessed after testing of a sample of the product in the applicant’s in-house laboratory and / or in an accredited independent laboratory for all the requirements as per relevant Indian Standard) and a copy of the test report(s), so generated, is(are) attached with application;

e) Agrees to comply with requirements laid down in a document, called “Scheme of Testing & Inspection (STI)”’. This STI (different for different Indian Standards) includes frequency of inspection and testing for various characteristics of the Indian Standard, which, as a part of process control, are required to be carried out by the licensee after the grant of BIS licence and appropriate records maintained. Copies of STIs are available with BIS and can be obtained at any time on request.
and / or at the time of submission or recording of application or during the visits by BIS inspecting officers.\textsuperscript{723}

After an application has been received by BIS a preliminary inspection is carried out at the applicant’s manufacturing and testing addresses and the competence of the application will be check with respect to:

a) availability of requisite in-house manufacturing and testing facilities as per the relevant Indian Standard(s);

b) competence of permanently employed testing personnel; and

c) conformity of the product sample(s) to the relevant requirements of the Indian Standard, when checked in the applicant’s factory during the preliminary inspection.\textsuperscript{724}

The BIS licence is granted to an applicant, if:

a) the results of preliminary inspection carried out by BIS officers are satisfactory,

b) the samples drawn during the preliminary inspection for independent testing are found conforming to the relevant Indian Standards for all the requirements, and

c) the applicant agrees to comply with requirements given in the relevant STI,

d) the applicant agrees to pay the annual minimum marking fee and the licence fee to BIS, and

e) the applicant agrees to enter into an Agreement with BIS for due compliance of the terms and conditions of the licence as given in Regulation 5 of the BIS (Certification) Regulations, 1988.\textsuperscript{725}

The initial licence is valid for one year and can be renewed for one or two years thereafter subject to ongoing satisfactory operation, as observed during BIS surveillance inspections. The conformity of factory and market samples to the relevant Indian Standard in independent testing is also verified.

**Systems Certification**

BIS has operated a Management Systems Certification Scheme since 1991. The following certification schemes are provided by BIS:

- Quality Management System Certification (IS/ISO 9001)

\textsuperscript{723} Procedure for Grant and Operation of BIS Licence under Foreign Manufacturers Certification Scheme (FMCS), no date. 
[http://www.bis.org.in/cert/fm.htm](http://www.bis.org.in/cert/fm.htm)

\textsuperscript{724} FMCS, op. cit., no date.

\textsuperscript{725} FMCS, op. cit., no date.
• Environmental Management System Certification (IS/ISO 14001)
• Hazards Analysis and Critical Control Point Certification (IS 15000)
• Occupational Health and Safety Management System (IS 18001)
• Food Safety Management System (IS/ISO 22000), Quality Management Systems - Requirements for service quality by public service organizations (IS 15700)
• Energy Management System Certification (IS/ISO 50001)

Furthermore, a scheme for Systems Certification against Indian Standards on Process, Services and Management Systems through BIS recognized Certification Bodies operating in India has recently been launched.

With regard to security products, systems and services it is evident that such entities will be certified by BIS according to relevant standards, although this is not clarified as a process or an option on the bureau’s website. A press release from the company Suprema, which produces biometric technology, outlines that the BIS certified its biometric scanners in June 2014. According to the press release these are the first biometric scanners to receive certification from BIS.

**Standardisation, Testing and Quality Certification (STQC)**

Standardisation Testing and Quality Certification (STQC) Directorate falls under the governmental Department of Electronics and Information Technology (DeitY) and provides quality assurance services, including testing, calibration, IT & e-governance, training and certification to public and private organisations.

In the area of IT & e-Governance, STQC provides assurance services through its IT Centres for Software Quality testing, Information Security and IT Service Management by conducting testing, training, audit and certifications.

STQC Certification Services took lead and became the first Third Party Certification Agency of domestic origin in India in 1991 to offer QMS certification. Since then STQC Certification Services has broaden its scope and is now providing Certification Service in QMS Product Certification/ISMS/ITSM/website quality / smart card / biometric devices along with a host of other schemes. It caters to the need of third party certification for the products in line with National and International standards and schemes. STQC offers certification services, to industry and other organisations, within the following fields:

**Management System Certification Schemes**

- ISO 9001 Quality Management System (QMS) Certification

---

729 STQC, op. cit., 2011b.
Product Certification Schemes

- Product Safety Certification based on IEC Standards (S mark)
- IECEE-CB Certification Based on IEC Standards
- Agency Inspection Services

Management System, Product Certification (IT & e-Gov)

- ISO 27001 Information Security Management System (ISMS) Certification
- ISO 20000-1 IT Service Management (ITSM) Certification
- Website Quality Certification
- Common Criteria Certification
- Smart Card Testing and Certification
- Biometric Devices Testing and Certification
- Software & System Certification.

In addition, STQC also certifies according to the Indian Common Criteria Certification Scheme (IC3S), which was established by the Department of Electronics and Information Technology (DEITY) as part of Cyber Security Assurance initiatives of the Government of India. "The purpose of the scheme is to evaluate and certify IT Security Products and Protection Profiles (PP) against the requirements of Common Criteria Standards ver. 3.1 at assurance levels EAL 1 through 4." The scheme provides National Certification, once Common Criteria Recognition Arrangement (CCRA) assessment is through and will also provide a framework for international certification through the International Mutual Recognition Arrangement with the other member countries of CCRA. Participation in this scheme is strictly voluntary unless it is mandated by government policy and/or regulations. STQC has the ultimate responsibility for the operation of the scheme in accordance with its policies and procedures as per the requirements of ISO/IEC Guide 65 (General Requirements for Bodies Operating Product Certification Systems). The scheme has the following objectives:

---

730 A "PP" is a document, typically created by a user or user community, which identifies security requirements for a class of security devices relevant to that user for a particular purpose. Common Criteria Portal of India, no date. http://www.commoncriteria-india.gov.in/Pages/FAQ.aspx

731 The Common Criteria for Information Technology Security Evaluation (CC) is an international standard (ISO/IEC 15408) for computer security certification and is currently in version 3.1. In this framework, computer system users can specify their security functional and assurance requirements, vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner. Common Criteria Portal of India, no date. http://www.commoncriteria-india.gov.in/Documentation/Scheme%20Documents/D01-CC%20Scheme%20Organization%20Management%20and%20Operations.pdf


733 There is a Common Criteria Mutual Recognition Arrangement (CCMRA) among participating countries, whereby each country thereto recognizes evaluations against the Common Criteria standard done by other countries.

734 India is a member of CCRA as a Certificate authorizing nation. As per the article 1 of the CCRA, Certificates issued by one member countries are accepted in other countries without re-certification. Only Government Body can be the Certification Body of the country and in India DEITY/STQC is the certification body.

To meet the needs of government and industry for cost-effective evaluation of IT products;

To encourage the formation of commercial security testing laboratories;

To ensure that security evaluations of IT products are performed to consistent standards;

To improve the availability of evaluated IT products.\textsuperscript{736}

Two types of security requirements are evaluated under the IC3S scheme:

- **Functional requirements**, which describe the desired security services to be provided by an IT product; and

- **Assurance requirements**, “which are expressed in the form of Evaluation Assurance Levels (EAL) a set of 7 hierarchical levels defined within the CC standard. CC evaluations that are certified in India (up to EAL4) shall be recognized by member of countries that are signatories to the Arrangement on the Recognition of Common Criteria Certificates (CCRA) after successful CCRA audit”\textsuperscript{737}

CC evaluation is an impartial assessment of an IT product by an independent body, and gives users confidence in its security functionality and provides them with a metric to compare the security capabilities of products with other products on the market. Certification provides independent confirmation of the validity of evaluation results, and thereby ensures comparability of these results across all evaluations under the scheme and facilitates mutual recognition of results between national schemes. Certification confirms that the product needs its security target to the claimed assurance level and that the evaluation has been conducted in accordance with the Standard of the scheme i.e. Common Criteria (e.g.: ISO 15408).\textsuperscript{738}

STQC and CC approved test laboratories (CCTLs) conduct security evaluations of IT products and protection profiles using STQC-approved test methods derived from the Common Criteria, Common Evaluation Methodology and other technology-based sources. The CCTL also has to demonstrate to the satisfaction of STQC that it is technically competent in the specific field of IT security evaluation and that it is in a position to comply in full with the rules of the scheme concerned. The test labs conduct testing and evaluation on IT products according to the following standards:


Figure 10099 outlines the process of testing and certification according to the IC3S scheme:

\textsuperscript{736} STQC, op. cit., 2 May, 2013

\textsuperscript{737} STQC, op. cit., 2 May, 2013

\textsuperscript{738} STQC, op. cit., 2 May, 2013
Figure 100: Process for CC certification in India

More information on Common Criteria is given in chapter 7.8.4.
4.4.5. **SUMMARY AND CONCLUSION**

The previous sections presented an overview of the Indian security market, along with outlining the standardisation and certification landscape. It presents short profiles of key organisations within this complex system. The Indian security market consists mostly of electronic products and majority of security equipment is imported from Germany, US, UK and Japan. Most in demand are integrated systems and software, CCTV, smoke detectors and metal detectors.

The national standardisation body BIS has made efforts and continues to harmonise national standards with international norms and ISO standards. There are however still a number of national standards still in use. The Indian standardisation system is complex and is composite of various organisation, governmental bodies and Ministries. India’s participation in international standardisation (ISO, IEC, and ITU) is at inter-governmental level since standardisation is within the remit government ministries. BIS is comprised of representatives of industry, consumer organisations, science and research. Each governmental ministry can define regulations and policies in its area of competence. Furthermore, within a ministry, several departments may be involved in standards and regulations within their area of competence.

With regard to security standardisation specifically, three sectional committees were identified which focus on standardisation within the remits of: security equipment, information systems security and biometrics and alarms and electronic systems. The report outlines a number of standards from each committee as well as standards currently in draft. As can be seen, the majority of the listed standards are harmonised Indian standards.

With regard to certification, there are a number of CBs, which work within India and the report outlines two key CBs, their remit, schemes and processes. With regard to best practice example, the Common Criteria scheme is a recent addition to the certification landscape in India and provides national certification, once assessment is through and also provides framework for international certification through the International Mutual Recognition Arrangement with the other member countries of Common Criteria Scheme.

4.4.6. **REFERENCES**

Bureau of Indian Standards, *Procedure for Grant and Operation of BIS Licence under Foreign Manufacturers Certification Scheme (FMCS)*, no date.
http://www.bis.org.in/cert/fm.htm


http://www.bis.org.in/sf/pow/powlitd.pdf

Bureau of Indian Standards, *How Indian Standards are made*, no date.
http://www.bis.org.in/sf/pros_setting_std.asp


4.5. ISRAEL

4.5.1. INTRODUCTION

This chapter contains a case study of Israel’s security industry, specifically with regard to standardisation and certification of security products, systems and services. Through desk research and short telephone interviews with experts on Israeli market actions, a brief overview of Israel’s security industry as well as the security standardisation framework is provided by presenting key organisations and bodies and their function with regard to the Israeli security standardisation and certification landscape.739

4.5.2. SHORT DESCRIPTION OF THE ISRAEL SECURITY INDUSTRY

4.5.2.1. KEY FIGURES

National security is of high priority in Israel – certainly for historical reasons and due to the ongoing military and terrorist threats that are manifested in different ways (for instance suicide bombers between 2000 and 2005, missile attacks in 1991, rockets in the north and the south of the country and so forth).741

The security market in Israel is divided into two markets: Homeland Security and Homeland Defence. The Homeland security industry is a crucial by-product of the strong military and defence sector.742 In this context, Israel has implemented state of the art security solutions especially regarding cyber security.743

Future prospects predict a growth of the Homeland Security and Homeland Defence markets until 2018 by 81 percent. The security industry within Israel is in most instances self-reliant depending mainly on internal defence and information technologies.744 According to the Investment Promotion Centre, around 600 Israeli companies operated in the security sector on Technology, Products, IT & Software and Services in 2014 (sector division see Figure 101100).
The security industry in Israel, as well as the defence industry, was established in the late 1940s. However, Israel is not only concerned about national safety and security. Moreover, Israel is one of the largest defence and security equipment exporters: Roughly 350 security companies in Israel export their products around the world. Figures of 2012 speak about an export volume of roundabout US$ 7.5 bn which is an increase of 30 percent compared to the previous year (2011: US$ 5.8 bn).

The Israeli security technology is seen worldwide as influential and innovative:

“Israel’s technologies have a dual influence of first being superior innovations, meeting the newest technical threats with the most elegant and creative technical solutions. But also, Israel’s innovators set the bar very high for other technologies around the world. In other words, the products coming from Sweden, Germany, the United Kingdom, Asia and North America are all the better because of the example set by Israel.”

A distinct focus of the Homeland security market is on aviation security (affecting serious investments in infrastructure, operations, support). The Israeli market is also attractive, for

---

745 Investment Promotion Centre, op. cit., 2013.
746 The Israel Export & International Cooperation Institute, op. cit., 2010, p. 2.
747 The Israel Export & International Cooperation Institute, op. cit., 2010, p. 2; ECORYS NL, et al., op. cit., 2009, p. 47
749 Support means “securing modern cities, by integrating existing surveillance capabilities with highly sophisticated situational awareness, and the command and control centers that empower ‘safe city’ initiatives” (The Israel Export & International Cooperation Institute, op. cit., 2010, p. 2).
instance, for the German security industry; in this context there are several cooperation treaties between Israel and Germany.⁷⁵⁰

“Israel today has earned its worldwide reputation for providing leading security solutions and continues to successfully partner with key world players to protect airports, seaports, government offices, financial institutions, recreational centers, international events and more.”⁷⁵¹

Israeli companies lead the field of border security: electronic fencing and covert “virtual fences”, backed by video motion detection capabilities, radar, electro-optical-based surveillance sensors, autonomous, unmanned aerial, ground and maritime patrol vehicles.⁷⁵²

Fields of expertise.⁷⁵³

- border protection⁷⁵⁴ and surveillance;
- virtual and physical perimeter protection systems for land-based and maritime sites;
- inspection systems for vehicle and cargo scanning at border crossings, airports, and seaports;
- countermeasures against potential terror attacks;
- IED/remote control bomb jammers;
- explosive ordnance disposal measures;
- ballistic armor protection;
- riot control solutions;
- non-lethal measures for law enforcement etc.

Key sectors:⁷⁵⁵

- Aviation, Maritime & Land Transportation Security (for example active and passive protection for aircraft, surveillance, access control, virtual fences for perimeter security, protection of facilities and assets on land);
- Safe Cities (control and communication networks, utilizing digital maps and geographical information systems (GIS); advanced image processing; human face recognition; video motion detection requirements; enhancing surveillance; security expertise by consultant and service providers);
- Force Protection;
- Chemical, Biological and Radiological (CBRN) Preparedness (Israel’s systems are stated as the world’s most advanced and widely used systems);⁷⁵⁶
- Command, Control & Communications;
- Counter Terror & Law Enforcement;

---


⁷⁵¹ Hunt, Steve, op. cit., no date.

⁷⁵² The Israel Export & International Cooperation Institute, op. cit., 2010, p. 4.

⁷⁵³ The Israel Export & International Cooperation Institute, op. cit., 2010, p. 3.

⁷⁵⁴ In the 1960s initial investments in border security, surveillance, route clearing and patrols were made.

⁷⁵⁵ The Israel Export & International Cooperation Institute, op. cit., 2010, p. 4-6.

⁷⁵⁶ Israel operates a Center for Counter CBRN Terrorism. This Center offers risk assessment, develop guidelines and training for emergency services (The Israel Export & International Cooperation Institute, op. cit., 2010, p. 5).
• Crisis & Emergency Management;
• Critical Infrastructure Protection (protection by physical obstacles such as fences and/or virtual obstacles such as electro-optical, radar, seismic or magnetic sensors etc.);
• IT Security & Anti-Fraud.

4.5.2.2. Cyber security strategy of Israel

Israel is seen as global leader in cyber security setting global standards in this field. The government of Israel is interacting directly with the private sector, academia, and civil society on cyber security issues. Critical infrastructures are nowadays inevitably referred to the information infrastructure in terms of computerised elements. "An infrastructure is a system that combines various facilities and enables certain activities." Infrastructures are specified critical when it is expected that function disruption "would lead to a significant socio-economic crisis with the potential to undermine the stability of a society and thereby cause political, strategic, and security consequences." In this context, Tabansky (2011) is highlighting that various countries have offered alternative definitions of critical infrastructures mentioning in a footnote the U.S. Government definition on critical information infrastructure.

Critical infrastructures in general as it is stated by the European Commission include:

• Energy installations and networks (e.g. electrical power, oil and gas production, storage facilities and refineries, transmission and distribution system).
• Communications and Information Technology (e.g. telecommunications, broadcasting systems, software, hardware and networks including the Internet)
• Finance (e.g. banking, securities and investment)

---

57 In this context, Israel launched an Advanced Technologies Park at Ben Gurion University which act as an international centre of excellence for “cybernetics and cyber security” (Sugarman, Eli, “What the United States can learn from Israel about cybersecurity”, Forbes online, 10 July 2014. http://www.forbes.com/sites/elisugarman/2014/10/07/what-the-united-states-can-learn-from-israel-about-cybersecurity; see also http://www.atp-israel.com/).
59 Tabansky, Lior, op. cit., 2011, p. 62; see also the definition of critical infrastructures by the European Commission: “Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. Critical infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services. Some critical elements in these sectors are not strictly speaking ‘infrastructure’, but are in fact, networks or supply chains that support the delivery of an essential product or service. For example the supply of food or water to our major urban areas is dependent on some key facilities, but also a complex network of producers, processors, manufacturers, distributors and retailers” (Eur-Lex, “52004DC0702 Communication from the Commission to the Council and the European Parliament – Critical Infrastructure Protection in the fight against terrorism”, no date http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0702:EN:HTML).
60 Tabansky, Lior, op. cit., 2011, p. 75: “Critical information infrastructures are systems and facilities whose destruction of interference (by means of computers) would: a. cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction; b. impair Federal departments and agencies’ abilities to perform essential missions, or to ensure the public’s health and safety; c. undermine State and local government capacities to maintain order and to deliver minimum essential public services; g. damage the private sector’s capability to ensure the orderly functioning of the economy through the cascading disruption of other critical infrastructure and key resources; or f. undermine the public’s morale and confidence in our national economic and political institutions’. U.S. Government, White House, Homeland Security, Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003”.
• Health Care (e.g. hospitals, health care and blood supply facilities, laboratories and pharmaceuticals, search and rescue, emergency services)
• Food (e.g. safety, production means, wholesale distribution and food industry)
• Water (e.g. dams, storage, treatment and networks)
• Transport (e.g. airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems)
• Production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials)
• Government (e.g. critical services, facilities, information networks, assets and key national sites and monuments).

Being essential, critical infrastructures are fundamental targets during conflicts. On this account, states, organisations, industries are constantly strive towards critical infrastructure protection by evolving up-to-date defence systems for their infrastructures: camouflage, guarding, fortification, defensive forces, deterrence etc.\textsuperscript{762}

Cyber security, which means also securing sensitive information and protecting computerised infrastructures, is an official issue in Israel since the second half of the 1990s (Cabinet decisions on the defence of cyber threats).\textsuperscript{763} On December 11 in 2002, the Ministerial Committee on National Security passed a decision on the “Responsibility for protecting computerized systems in the State of Israel”, which serves from this day on as Israeli response towards cyber threats to critical information infrastructure. Within the scope of the ministerial decision a steering committee and a government unit, the Information Security Agency, was established.\textsuperscript{764} It is not startling, that guidelines on protecting critical infrastructures are not publicly available in Israel, as an interviewed expert also stated.

According to an expert, national regulation on cyber security are important for security standardisation activities in Israel. In this context, current standardisation projects in the field of security are on mapping and adopting international standards pertaining to cyber security.

4.5.3. \textbf{THE SECURITY STANDARDISATION FRAMEWORK AND RELEVANT REGULATIONS}

The most Israeli standards are on a voluntary basis although they might become mandatory standards whenever they are of crucial importance for the protection of public safety, health or the quality of life.\textsuperscript{765}

\textsuperscript{762} Tabansky, Lior, op. cit., 2011, p. 62.
\textsuperscript{763} Tabansky, Lior, op. cit., 2011, p. 72.
4.5.3.1. **The Standards Institution of Israel**

The Standards Institution of Israel (SII) is the country’s national public, non-profit statutory standards institution mandated by the Israeli Government and empowered by the Standards Law of 1953.\(^{766}\) SII prepares and publishes Israeli standards and represents Israel in the international standards organisations – the International Organization for Standardization (ISO\(^{767}\)) and the International Electrotechnical Commission (IEC\(^{768}\)). SII is operating in three main areas: Standardisation, Testing and Certification. More than 3,000 Israeli standards have been published so far. According to SII, activities on standardisation are organised in 17 diverse areas. The development of a standard at the SII follows a five steps process (see Figure 102).

![Diagram of standardisation process](http://www.sii.org.il/1005-en/SII_EN.aspx)

**Source:** Own figure based on SII b\(^ {769}\)

Figure 102: Initiating and approving standards in Israel

The SII also operates product and system certification programmes. These certification programmes include three marking schemes: Standards Mark, Safety Mark, and Green Label.\(^ {770}\) However, there is a trend to adopt European standards in Israel. Israeli legislation mandates the adoption of multiple, proven international standards if possible in order to fix the retention benefits to the Israeli consumers of competitive markets. In this context, the SII became an affiliate of the European Committee for Electrotechnical Standardisation (CENELEC).\(^ {771}\)

4.5.3.2. **Israel’s ISO Participation**

The SII is participating in selected security-related ISO Technical Committees (see Figure 103102):

---


\(^{767}\)ISO is an independent, non-governmental membership organisation. SII is a founding member of ISO (ISO b, op. cit.).


\(^{770}\)For the marking schemes see: https://portal.sii.org.il/eng/qualityauth/teken-lobby.aspx.

### 4.5.4. THE SECURITY CONFORMITY ASSESSMENT FRAMEWORK

#### 4.5.4.1. CONFORMITY ASSESSMENT IN ISRAEL IN GENERAL

The Israel Accreditation Authority

The Israel Laboratory Accreditation Authority (ISRAC) is the only statutory body in Israel. ISRAC was established under the Law of the Israel Laboratory Accreditation Authority in 1997 and functions as authority “to provide recognition of the ability and professional competence of laboratories to perform tests in accordance with the world standards, regulations, and other reference specifications.” The basics for their actions are the ISO/IEC 17011 guide-

---

ISO TC | Topic | Participation (P/ O-Member) |  
--- | --- | --- |  
ISO/IEC/JTC 1/SC 17 | Cards and personal identification | P |  
ISO/IEC/JTC 1/SC 27 | Information technology - security techniques | P |  
ISO/IEC JTC 1/SC 31 | Automatic identification and data capture techniques | P |  
ISO/IEC/JTC 1/SC 37 | Biometrics | P |  
ISO/TC 85 | Nuclear energy, nuclear technologies, and radiological protection | - |  
ISO/TC 92 | Fire safety | O |  
ISO/TC 223 | Societal security | P |  
ISO/TC 224 | Service activities relating to drinking water supply systems and wastewater systems - Quality criteria of the service and performance indicators | P |  
ISO/TC 247 | Fraud countermeasures and controls | O |  
ISO/PC 284 | Management system for quality of private security company (PSC) operations - Requirements with guidance | O |  
ISO/TC 292 | Security | P |  
Total P+O | | 7+3 |  

Source: ISOa

Figure 103: Israel’s involvement in selected security-related ISO TCs

---


773 ISO a, “Participation in TCs: Israel (SII)”, no date. http://www.iso.org/iso/home/about/iso_members/iso_member_participation_tc.htm?member_id=1819

lines defining the operating method of accreditation bodies.\textsuperscript{775} ISRAC is a full recognised member of the International Laboratory Accreditation Cooperation (ILAC) and has signed mutual recognition agreements with ILAC and the European Accreditation (EA).\textsuperscript{776} ISRAC has accredited laboratories in the areas of: food, water, cosmetics, pesticide chemistry, biology, microbiology as well as many calibration, engineering, construction laboratories NDT (non-destructive testing) and EMC (telecommunications).\textsuperscript{777} Accreditation operated by ISRAC is a five-step process (see Figure 104103):

\begin{figure}[h]
\centering
\begin{tabular}{c}
\textbf{Request for accreditation} & \textbf{Accreditation consent} & \textbf{Assessment preparation} & \textbf{Assessment performance} & \textbf{Accreditation certificate publication}
\end{tabular}
\caption{Accreditation process by ISRAC}
\end{figure}

Source: Own figure based on ISRAC\textsuperscript{c}\textsuperscript{778}

The Institute of Quality & Control: An Israeli Certification Body

The Institute of Quality & Control (IQC) is the largest private CB in Israel founded in 1959 by the Ministry of Industry & Commerce and the Manufacturers Association of Israel. The IQC was privatised starting in 2008. Common standards of the IQC include (Figure 105104):

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 9001</td>
<td>Quality management systems</td>
</tr>
<tr>
<td>ISO 14001</td>
<td>Environmental management systems</td>
</tr>
<tr>
<td>ISO 22000</td>
<td>Food safety management systems</td>
</tr>
<tr>
<td>OHSAS 18001</td>
<td>Occupational Health and Safety Assessment Series</td>
</tr>
<tr>
<td>ISO 13485</td>
<td>Medical devices</td>
</tr>
<tr>
<td>ISO 27001</td>
<td>Information technology</td>
</tr>
<tr>
<td>AS 9100</td>
<td>Aerospace Standard</td>
</tr>
<tr>
<td>SA 8000</td>
<td>Social Accountability</td>
</tr>
<tr>
<td>ISO 22716</td>
<td>Cosmetics</td>
</tr>
</tbody>
</table>

Source: IQC, “Standards & certification”, no date. [http://www.iqc.co.il/?categoryId=87288](http://www.iqc.co.il/?categoryId=87288).

However, according to an expert, the IQC is not the responsible institution for the certification of security technologies and products in Israel. Information about respective Israeli bodies remain unanswered.

\textsuperscript{775} ISRAC a, op. cit., no date.


4.5.4.2. Conformity Assessment Framework in the Security Field

The SII is also a consuming member of the Common Criteria Recognition Arrangement (CCRA), an arrangement in order to ensure that the evaluations of Information Technology products and protection profiles are performed to high and consistent standards. Furthermore, the SII has for example signed mutual recognition agreements with organisations from the United States such as follows (see Figure 106105):

<table>
<thead>
<tr>
<th>Department of Defence</th>
<th>QPL ANS QML for Electronic components</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETL (by Intertek)</td>
<td>Standards Mark recognition – Electrical and energy products</td>
</tr>
<tr>
<td>FCC (Federal Communications Commission)</td>
<td>Recognition</td>
</tr>
<tr>
<td>IAPMO (International Association of Plumbing and Mechanical Officials)</td>
<td>Hydraulic products Standards Mark</td>
</tr>
<tr>
<td>NFS (Public Health and Safety Organization)</td>
<td>Food safety, HACCP-9000, HACCP</td>
</tr>
<tr>
<td>UL (global independent safety science company)</td>
<td>Mutual recognition in fields of: Electricity, electronics, hydraulics, mechanics, fire. Standards Mark supervision in fields of: Electricity, electronics, hydraulics, mechanics, fire</td>
</tr>
</tbody>
</table>

Figure 106: Mutual Recognition Agreements between SII and U.S. organisations

The ETL mark, for instance, as well as the UL mark, are two of the most important security certificates in the USA. Furthermore, there seem to be testing centres which are working on behalf of the Israeli government. For instance, in 2012 a “next-generation” of body scanner, the Ait84 model scanner, for use at Israeli airports have been developed and tested (ISA testing) at the Ben-Gurion Airport.

4.5.5. Summary and Conclusions

Security and security solutions are considered a high priority in Israel. Accordingly, Israel has implemented state of the art security solutions, particularly in the field of cyber security. As such, Israeli security technologies are considered both influential and innovative, indicating that Israeli approaches and expertise can be integrated or proposed within certification and

---

standardisation boards. A singular statutory standards institution (SII) is involved in security-related ISO Technical Committees, as well as the operating product and system certification programs. SII asserts that it follows a policy of standard harmonisation whenever possible, meaning that existing and accepted international standards are adopted as Israeli standards, such as the CE marking, if no local regulations that say otherwise. There have also been occasions when specifications created in Israel have been adopted by the international community.

4.5.6. REFERENCES


ECORYS NL, DECISION Études et Conseil and TNO, Study on the Competitiveness of the EU security industry. Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054, 15 November 2009.


785 SII a, op. cit., 2014.
Intertek, “Certification”, no date. 
http://www.intertek.com/life-safety/certifications/etl/


IQC – Institute of Quality & Control, “Standards & certification”, no date. 
http://www.iqc.co.il/?categoryId=87288


ISO a– International Organization for Standardization, “Participation in TCs: Israel (SII)”, no date. 
http://www.iso.org/iso/home/about/iso_members/iso_member_participation_tc.htm?member_id=1819

http://www.iso.org/iso/home/about/iso_members/iso_member_body.htm?member_id=1819


ISRAC a – Israel Laboratory Accreditation Authority, “From ISRAC”, no date. 
http://www.israc.gov.il/?CategoryID=249

ISRAC b – Israel Laboratory Accreditation Authority, “International activity”, no date. 
http://www.israc.gov.il/?CategoryID=255

ISRAC c – Israel Laboratory Accreditation Authority, “The Accreditation Process”, no date. 
http://www.israc.gov.il/?CategoryID=306

http://www.keystonecompliance.com/israel/

Reuters, “Israel Approves Next-Generation Body Scanner From Tek84 Engineering Group”, 
9 August 2012. 


SII a – Standards Institution of Israel, “Standards“, no date. 


TASE – Tel Aviv Stock Exchange, “Israel Securities Authority”, no date. http://www.tase.co.il/Eng/AboutTASE/RegulationInIsrael/IsraelSecuritiesAuthority/Pages/IsraelSecuritiesAuthority.aspx


4.6. JAPAN

4.6.1. INTRODUCTION

Economically, Japan is one of the most highly developed industrial nations in the world, and is currently the EU’s 7th most important trade partner, with a yearly total trade volume of €116 bn²⁸⁶ (3.6% of EU trade). Its major export industries are automobiles, consumer electronics, and computers, semiconductors, copper, iron, and steel. Additional industries include petrochemicals, pharmaceuticals, bio industry, shipbuilding, aerospace, robotics, textiles, and processed foods.

Japan established its first unified national system of industrial standardisation - the JESC (the Japanese Engineering Standards Committee) in 1921.²⁸⁷ The JESC committee undertook the adoption of national standards (JES). Then in 1945 (after WWII) and under the influence of the United States, the present Japanese Standards Association (JSA²⁸⁸) was established, the Industrial Standardisation Law was promulgated, and the Japanese Industrial Standards Committee (JISC²⁸⁹) was set up, as an advisory organisation to competent Ministers in charge of the elaboration of Japanese Industrial Standards (JIS).

JISC is tasked with specifying the standards used for industrial activities in Japan, and publishes the standards through the JSA. It is also Japan’s representative in both ISO²⁹⁰ and IEC.²⁹¹ There are currently over 10,000 JIS standards for business and manufacturing processes in Japan. The designation (logo) for the JIS Mark is as pictured:

![JIS logo](source: JIS Figure 107: JIS logo)

4.6.2. JAPAN’S SECURITY INDUSTRY

The overall size of the Japanese security market is US$ 6.3 bn (around € 5.6 bn), including equipment and services and the market is projected to grow by three percent a year for the

²⁸⁷ ISO, Profile page for Member Body JISC, no date. http://www.iso.org/iso/about/iso_members/iso_member_body.htm?member_id=1835
²⁹⁰ ISO, op. cit., no date.
next few years. There are approximately 9,000 security firms in Japan, although most of them are of small scale. The two biggest security companies are Secom and ALSOK. The main focus of the majority of these security companies appears to be on stationed security services and traffic control services, and having close business relationships with regional communities.

**Secom Co., Ltd.** was established in 1962 as the first private security company in the country, and now has approximately 200 operations in Japan, United States, United Kingdom, Australia, New Zealand, South Korea, Taiwan, China, Thailand, Vietnam, Malaysia, Singapore, and Indonesia, with total yearly revenue of about € 2.7 bn. The company describes itself as “a pioneer and leader of security services in Japan”. They offer centralised (on-line) security systems, self-contained (off-line) security systems, security products, and other security services.

Their security products include access-control systems, closed-circuit television (CCTV) systems, automated fire detection and extinguishing systems, and internal and external monitoring systems that can be used alone or connected to on-line security systems. Other services include a static guard service and amorded car services.

Their centralised (on-line) security systems come configured with on-site sensors and controllers that detect intruders, fires and equipment malfunctions that are linked to control centers, where they are constantly monitored. In case of an emergency, response personnel are available.

**Sohgo Security Services Co., Ltd. or ALSOK** (“Always Security OK”) was founded in 1965 and is headquartered in Tokyo, Japan. They provide electronic security, stationed security, transportation security, and total management services in Japan. They are organised into several segments, namely: electronic security services, stationed security services, transporta-

http://export.gov/build/groups/public/@eg_main/@byind/@security/documents/webcontent/eg_main_060212.pdf  
http://www.alsok.co.jp/en/ir/faq/  
795 Secom corporate website, 2015.  
http://www.secom.co.jp/english/  
796 Secom, “Security Services for the business scenes”, no date.  
http://www.secom.co.jp/english/business.html  
797 Secom, op. cit., no date.  
798 Secom, op. cit., no date.  
tity persons who enter or exit the facilities. They conduct regular patrols to detect irregularities. ALSOK also offers services in Transportation Security Services segment that include catering to ATMs and cash deposit machines stationed inside banks, convenience stores, and other venues. They transport cash and other valuables, and offer an online system so that operators can track daily revenues. Lastly, in the Total Building Management and Disaster Prevention Services segment ALSOK offers various services for large property owners such as property management, cleaning and maintenance, security. They also sell and install fire extinguishing equipment.\(^{800}\)

As for their Security Robot segment, ALSOK claim to be a nation leader in their field. They began their research and development activities on security robots in 1982. In December 2006, ALSOK launched “Reborg-Q,” a new security system that combines security guards with robots, the robots overseeing those tasks that machines can perform better than humans. A recent addition is the use of face recognition technology, which instantly alerts security guards if a robot recognizes a pre-registered face in an unauthorized area.\(^{801}\)

ALSOK acquired certification under the ISO 9001 standard for quality management systems in September 2002. 50 of the ALSOK group members have acquired ISO 9001 accreditation as of September 30, 2012.\(^{802}\) The company issues reports on its CSR activities based on ISO 26000, an international standard for social responsibility, and has acquired a PrivacyMark certification in July 2013.\(^{803}\) The PrivacyMark certification as well as many other certificates and standards relevant in the CRISP context are described in the following chapters.

### 4.6.3. Security Standardisation Framework

The present Japanese Standards Association (JSA) was established in 1945, much under U.S. guidance. The following year, the Japanese Industrial Standards Committee (JISC) and the Japanese standards framework were formed. Then in 1949, the Industrial Standardisation Law was enacted, forming the legal basis for the present Japanese Industrial Standards (JIS). The law was last revised in 2004, changing the JIS mark used for designating JIS-certified products. The new mark has been used for all new products since late 2008.\(^{804}\)

JIS standards are named in the form of "JIS X 0208:1997", where the letter in the beginning denotes the area division, in the present example Information Processing. It is followed by four digits (or five digits for those standards that correspond to existing ISO standards), and the year of the last revision. There are 19 division areas, dealing with the various industry areas, comprising a total of about 10,400 standards (see Figure 108107).

The process for developing a new JIS is as follows: firstly, the need for a new standard is identified within government or industry, and noted with JISC. Then, a JIS drafting committee is formed and tasked with producing a JIS draft. The finished draft is deliberated upon by

---

800 ALSOK, op. cit., 2015.
801 ALSOK, op. cit., 2015.
JISC, and then voted on. Once confirmed, it must then be formally confirmed by the relevant government Minister (depending on the standard’s field).\textsuperscript{805} The full process is illustrated in Figure 108.

\begin{table}[ht]
\centering
\begin{tabular}{|l|c|c|c|c|}
\hline
\textbf{JIS Sector} & \textbf{Type of promulgation} & \textbf{Newly Established} & \textbf{Revised} & \textbf{Withdrawn} & \textbf{Change in No. of Standards} & \textbf{Total} \\
\hline
A. Civil Engineering and Architecture & 4 & 31 & 104 & 8 & -4 & 571 \\
B. Mechanical Engineering & 15 & 53 & 204 & 15 & 0 & 1,651 \\
C. Electronic and Electrical Engineering & 43 & 39 & 166 & 8 & 35 & 1,601 \\
D. Automotive Engineering & 8 & 2 & 18 & 2 & 6 & 372 \\
E. Railway Engineering & 2 & 3 & 6 & 1 & 1 & 146 \\
F. Shipbuilding & 0 & 4 & 94 & 0 & 0 & 386 \\
G. Ferrous Materials and Metallurgy & 20 & 52 & 43 & 3 & 17 & 440 \\
H. Nonferrous Materials and Metallurgy & 2 & 29 & 27 & 1 & 1 & 410 \\
K. Chemical Engineering & 15 & 64 & 214 & 10 & 5 & 1,740 \\
L. Textile Engineering & 0 & 5 & 4 & 1 & -1 & 218 \\
M. Mining & 2 & 2 & 21 & 3 & -1 & 162 \\
P. Pulp and Paper & 8 & 0 & 14 & 3 & 5 & 77 \\
D. Management System & 2 & 6 & 0 & 0 & 2 & 80 \\
R. Ceramics & 17 & 5 & 81 & 0 & 17 & 371 \\
S. Domestic Wares & 1 & 6 & 3 & 0 & 1 & 190 \\
T. Medical Equipment and Safety Appliances & 17 & 38 & 41 & 0 & 17 & 526 \\
W. Aircraft and Aviation & 0 & 0 & 40 & 0 & 0 & 97 \\
X. Information Processing & 3 & 15 & 24 & 0 & 0 & 0 \\
Z. Miscellaneous & 11 & 28 & 113 & 2 & 9 & 836 \\
\hline
\textbf{Total} & 170 & 392 & 1,217 & 57 & 113 & 10,399 \\
\hline
\end{tabular}
\caption{Number of JIS revised or withdrawn in Fiscal Year 2012}
\end{table}

Source: JISC\textsuperscript{806}

Figure 108: Standardisation activities at JIS across industries

Source: JISC\textsuperscript{807}

Figure 109: JIS development process

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{jisc_diagram.png}
\caption{JIS development process}
\end{figure}

\textsuperscript{807} JISC, op. cit., 2011, p. 12
After promulgation, JIS standards are applied through Japanese laws and regulation. According to JISC data\(^{808}\), close to 200 Japanese laws apply JIS to technical regulations, citing a total of 1,306 JIS standards. Particularly interesting regulations in the security field appear to be:

- The Building Standards Act,
- The Industrial Safety and Health Act,
- The Act on the Regulation of Nuclear Source Material, Nuclear Fuel Material and Reactors.

JISC is also involved with international standards organisations ISO and IEC. In their view, harmonisation of Japanese national standards with appropriate international standards greatly facilitates the use of their products internationally, and in turn favors Japanese trade with their international partners. Additionally, JISC has done work on other international legislation pertaining to technical standards, such as harmonizing the national legislation with the provision of the GATT Standards Code, and later, the World Trade Organization’s TBTs (Technical Barriers to Trade).\(^{809}\)

Their activities include participation as a Participating (P) Member in Technical Committees (TCs), Sub-Committees (SCs) or Working Groups (WGs), as outlined below. Additionally, JISC is a member of the secretariat in 36 ISO, 11 IEC and 3 ISO/IEC (a total of 50) joint committees. Their role in this field has recently increased, although it still lags somewhat behind leading industrial nations in the EU and the USA.

In general, according to JISC data,\(^{810}\) of the 10,399 JIS standards in force at the end of 2012, 40% were identical to respective ISO/IEC standards, 57% were modified to some degree, and 3% were deemed non-equivalent or substantially different from their ISO/IEC counterparts. The same holds true in the security field. According to the data in the JIS standards database\(^{811}\), out of 48 JIS standards (both past and present) bearing the word “security” in their name, only 3 are not identical to an ISO/IEC counterpart\(^{812}\), and an additional 1 is modified\(^{813}\). In the area of security alarm standards, 3 out of 20 are identical, 6 modified\(^{814}\), and 11 aren’t based on an ISO/IEC counterpart standard.\(^{815}\) Thus, while Japanese security standards

---

\(^{808}\) JISC, op. cit., 2011, p. 16
\(^{810}\) JISC, op. cit., 2011, p. 9
\(^{812}\) JJS X5054 (Security technology - The digital signature scheme that allows for message recovery), X5091 (Security techniques - Security testing requirements of the cryptographic module), and X7012-4 (Government / industry information exchange for syntax rules (CII syntax rules) - Part 4: Security features).
\(^{813}\) JIS Q Q27000 (Information technology - Security techniques - Information security management systems), corresponding to ISO /IEC 27000:2014
\(^{814}\) JIS D0033 (Passenger cars - hand operation and weighing - warning device such placement), JIS D0035 (Two-wheeled motor vehicles - operating device, identification mark of the display device and warning device), JIS D0802 (Car - front vehicle collision warning devices - performance requirements and test procedures), JIS F0412 (Ship engine department equipment alarm and display of system), JIS X5774 (Open Systems Interconnection - System management - alarm reporting function), JJS X5777 (Open Systems Interconnection - System management - safety protection alarm reporting function).
\(^{815}\) JIS D3605 (Liquefied petroleum gas gas leak alarm for automobiles), JIS E3702 (Railroad crossing alarm for withdrawal indicator), JIS F0415 (Board layout design criteria of small marine Misao ‘s room Master machine (maneuvering stand and maneuvering plant)
still differ in some field, in general, the level of harmonisation with ISO/IEC is already quite high, while still growing. Note: the degree of correspondence of the standards is in line with international standards is in accordance with the definition of ISO/IEC Guide 21-1.

Below is a list of security-related ISO TCs in which JISC currently participates:

<table>
<thead>
<tr>
<th>ISO TC</th>
<th>Topic</th>
<th>Participation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC/JTC 1/SC 17</td>
<td>Cards and personal identification</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 21</td>
<td>Equipment for fire protection and fire fighting</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 27</td>
<td>IT Security techniques</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 31</td>
<td>Automatic identification and data capture techniques</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 36</td>
<td>Safety aspects and impact testing</td>
<td>P</td>
</tr>
<tr>
<td>ISO/IEC/JTC 1/SC 37</td>
<td>Biometrics</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 68</td>
<td>Financial Services</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 68/SC 2</td>
<td>Financial services, security</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 85</td>
<td>Nuclear energy, nuclear technologies, and radiological protection</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 92</td>
<td>Fire safety</td>
<td>P, secretary</td>
</tr>
<tr>
<td>ISO/TC 92/SC 1</td>
<td>Fire initiation and growth</td>
<td>P, secretary</td>
</tr>
<tr>
<td>ISO/TC 92/SC 2</td>
<td>Fire containment</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 92/SC 3</td>
<td>Fire threat to people and environment</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 92/SC 4</td>
<td>Fire safety engineering</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 94</td>
<td>Personal safety -- Protective clothing and equipment</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 199</td>
<td>Safety of Machinery</td>
<td>P</td>
</tr>
<tr>
<td>ISO/TC 262</td>
<td>Risk Management</td>
<td>P</td>
</tr>
</tbody>
</table>

Figure 110: Japan’s involvement in selected security-related ISO TCs
4.6.4. SECURITY CONFORMITY ASSESSMENT FRAMEWORK

Conformity assessment plays an important role in various areas in Japan, including safety control, government procurement, business transactions and product selection by consumers.

The Japanese Ministry of Economy, Trade and Industry (METI) is in charge of managing the JIS Mark Certification Scheme and ensuring mutual recognition with other countries.

In this respect, a new JIS Mark Certification Scheme (as pictured in Figure 106) was launched in October 2005 based on the revised Industrial Standardisation Act. The scheme is an internationally harmonised third-party certification system under which private-sector CBs conduct certification activities. METI has organised various initiatives to help bolster the mark, including “strict responses to factories that breach the rules, on-site inspections of certified business operators, inspections of purchased product samples, and regional seminars on JIS Mark Certification Scheme”. As of March 2010, the certification scheme covered approximately 2,100 standards, and approximately 8,800 certifications have been conducted.816

In addition, Japanese corporations are actively seeking certifications for international management system (MS) standards such as ISO 9001 (Quality), ISO/IEC 27001 (information security management) and ISO 14001 (Environment). As of 2013, about 37,000 organisations have received certification for ISO 9001 and about 20,000 for ISO 14001 nationwide.817

Furthermore, Japan Information Processing Development Center (JIPDEC) operates four conformity assessment schemes:

- ISMS (Information Security Management System), based on ISO/IEC 27001, a well-known certification scheme that allows organisations to systematically determine, manage and improve on their information security needs (using the standard PDCA – plan, do, check, act - model);818
- CSMS (Cyber Security Management System), based on IEC 62443-2-1, which provides certification for cyber security in industrial automation systems (IACS) supporting critical social and industrial infrastructure, in today’s age where both online and offline cyber threads have become a persistent reality;819
- ITSMS (Information Technology Service Management System), based on EC 20000-1, an international standard for quality management specifically focused around IT service management;820
- BCMS (Business Continuity Management System; see also section 2.6.6. below)821

These four schemes aim to promote information management systems based of international standards.

---

817 JISC, op. cit., 2013, p. 15.
821 JIPDEC, op. cit., no date.
Upon instruction from METI, JIPDEC established a PrivacyMark System, a certification for appropriate handling of personal information, available to private enterprises that is based on respect of all relevant laws, regulations and standards. The system follows the industry standard (JIS Q 15001 “Personal information protection management system - Requirements”). Such private enterprises are granted the right to display “PrivacyMark” in the course of their business activities. The system is in compliance with Japan Industrial Standards (JIS Q 15001:2006 Personal Information Protection Management System - Requirements). CABs that provide certification are accredited by JIPDEC.

However, there have been some challenges. As METI reports, several large organisations have been involved with (well-publicized) management-related scandals in the early 2000s, calling the credibility of the Japanese MS certification scheme in question. To counteract this, in 2008 METI published specific “Guidelines for the improvement of management system certification” targeting accreditation bodies, and then initiated an action plan called “Japan Initiative for Reliability Enhancement of Certification (JIREC)”. The plan has in recent years been well-accepted by the regional accreditation bodies such as the Asia Pacific Laboratory Accreditation Cooperation (APLAC) and their counterparts the Pacific Accreditation Cooperation (PAC) and the International Accreditation Forum (IAF). In the future, METI plans to step up their efforts in enhancing the scheme’s reliability and reputation, with measures such as on-site inspections of certified laboratories.

There are a number of accreditation bodies in Japan:

- **Japan Accreditation Board (JAB)** is established as a Public Interest Incorporated Foundation under authorisation from the Japanese Cabinet Office’s Public Interest Corporation Commission. JAB is a member of international MLA (Multilateral Recognition Arrangement) groups for the accreditation of quality and environmental management system certification bodies, and MRA (Mutual Recognition Arrangement) group for testing laboratories, and medical laboratories. JAB performs accreditation and registration of management system certification bodies and personnel certification bodies, of product certification bodies; greenhouse gas (GHG) validation and verification bodies; of laboratories, medical laboratories and inspection bodies; and evaluation service based on the MRA Law.

- **International Accreditation Japan (IAJapan)** as a governmental organisation established within the National Institute of Technology and Evaluation (NITE) with the aim to accredit testing laboratories, calibration laboratories, product certification bodies, reference material producers according to the international standards to support the reliability of data in testing and calibration as well as the quality of product.

---

824 The full list of the Privacy Mark Conforminity Assessment Bodies is available at http://privacymark.org/agency/member_list.html.
825 JISC, op. cit., 2013, p. 15
826 A full list is available at IAF members and signatories, no date. http://www.iaf.nu/articles/IAF_MEM_Japan/85
827 JAB, Outline, no date. http://www.jab.or.jp/en/about/profile/
Japan Accreditation System for Product Certification Bodies of JIS Mark – JISC accredits certification bodies that carry out examinations based on applicable JIS standards.\(^{829}\)

As shown before, JIPDEC provides additional accreditation for the certification bodies which use its certification scheme.

METI also set up the Japan National Laboratory Accreditation System (JNLA) in order to accredit testing laboratories, ensuring they are able to use appropriate testing methods as per JIS, and in turn issue reliable testing reports. Accredited laboratories get to issue test reports including the JNLA logo. Additionally, through international cooperation with the Asia Pacific Laboratory Accreditation Cooperation (APLAC), METI has ensured their test certificates are widely internationally accepted. As of March 2013, 210 testing laboratories have been accredited by JNLA, altogether issuing approximately 200,000 test reports annually.\(^{830}\)

### 4.6.5. Selected Security Certification Bodies and Their Work

This chapter provides information on three CABs / certification schemes, relevant for the Japanese market for security solutions.\(^{831}\)

- Bureau Veritas Japan (global CB)
- GIC - Guardian Independent Certification Japan (global CB)
- Japanese Information Technology Security Evaluation and Certification Scheme ("JISEC")

Created in 1828, **Bureau Veritas** is one of the leading global companies in the areas of Testing, Inspection and Certification (TIC). They offer services and solutions to ensure that their clients’ products, infrastructure and processes meet the required national and international standards in terms of quality, health, safety, environmental protection and social responsibility. Their work is divided into eight different divisions: marine and offshore (their original business), industry, construction, in-service inspection and validation, certification, commodities, consumer products, and government services & international trade. They provide certification in several security-related fields, including ISO 20000-1 and 27001 (information services, security), OHSAS 18001 (occupational health and safety), ISO 39001 (road safety), etc. As of late 2014, the group included over 1,400 offices and laboratories in over 140 countries. Their Japanese subsidiary is based in Yokohama.\(^{832}\)

---

GIC - Guardian Independent Certification is a global CB with an ISO/IEC 27006:2011 certification for Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems. They operate an office in Tokyo.

Japanese Information Technology Security Evaluation and Certification Scheme ("JISEC") offers IT product security certification in accordance with ISO/IEC 15408, the international standard for evaluation criteria for IT security. Certification is currently being conducted by the Information-technology Promotion Agency, Japan ("IPA"). IPA operates JISEC from the standpoint of the Certification Body and is also involved in overseeing the scheme and engaging in international collaboration.835

ISA Security Compliance Institute was founded in 2007 and aims to provide the highest level of assurance for information and cyber security of industrial automation control system. They achieve this through industry standards compliance programs, education, technical support, and life-cycle management. Their original members include Chevron, ExxonMobil Research and Engineering, Honeywell, Invensys, Siemens, and Yokogawa.834

4.6.6. RECENT DEVELOPMENTS AND CURRENT SECURITY MARKET TRENDS

In the aftermath of the Fukushima nuclear power plant disaster, many Japanese trading firms are reconsidering their existing Business Continuity Planning (BCP), and are carrying more radiation protective products and detector equipment. Thus, the market for radiation protection-related products has become highly competitive. The market for personal protective equipment for workers and new technologies capable of treating contaminated soil is also expected to show growth.

Furthermore, cloud computing services for data backup have attracted considerable attention because many Japanese companies experienced losses of vital data and systems from damage caused by the devastating earthquake and tsunami.835

4.6.7. IDENTIFICATION OF GOOD PRACTICES APPROACHES

An interesting aspect of Japan’s standardisation strategy is the fact the both JISC and METI have been making various efforts to improve their international standardisation activities, such as by conducting regular consultation meetings on a bilateral basis.836 Other interesting examples are METI’s “Guide for the improvement of (management system) certification” and the “Japan Initiative for Reliability Enhancement of Certification (JIREC)”.

836 JISC, op. cit., 2013, p. 17
Japan has also held regular information exchange meetings (once a year) since 1996 with CENELEC and the two organisations signed a Memorandum of Understanding (MoU) in 2005. In November 2012, the 5th information exchange meeting based on the MoU was held concurrently with JISC-CENELEC information exchange meeting in Brussels, Belgium. A similar MoU was signed with CEN.

In addition, a governmental bilateral EU-Japan Working Group on standards and conformity assessment exists under the EU-Japan Industrial Policy and Industrial Cooperation Dialogue.

Regarding specific security aspects, Japan responded to the Fukushima power plant disaster by increasing its efforts in nuclear security, which has led to a growing market in that segment. Their specific efforts may lead to new and advanced knowledge, which may specifically enrich international standardisation in this field.

4.6.8. SUMMARvY AND CONCLUSION

Japan views its international standardisation activities as critical for achieving further economic recovery and growth, and enhancing its competitiveness in global markets. Standardisation is entrusted to the Japanese Industrial Standards Committee (JISC), which maintains new and existing Japanese industrial standards (JIS), and in particular, strives to ensure their compatibility with respective international standards through their participation in respective ISO/IEC TCs. Based on an estimate on their part, 40% of JIS standards are currently identical to respective ISO/IEC standards, 57% were modified to some degree, and 3% were deemed non-equivalent or substantially different. An even greater ratio is expected to become identical in due future. Particularly important in this is the continued technical cooperation between Japanese and EU authorities in the CENELEC, CEN and a bilateral bilateral EU-Japan CA working group.

With the aim of improving the credibility of Japanese certification schemes METI recently published specific “Guidelines for the improvement of management system certification” and then initiated an action plan called “Japan Initiative for Reliability Enhancement of Certification (JIREC)” targeted at the accreditation bodies in Japan that was well accepted by regional accreditation organisations. The latest developments follow the Fukushima power plant disaster, which lead to a growing market in nuclear security.

4.6.9. REFERENCES


838 JISC, op. cit., 2013
839 JISC, op. cit., 2013, p. 13
Always Security OK, (ALSOK), *CSR Report 2012*.  

Always Security OK, (ALSOK), *Annual report 2013*,  

Bureau Veritas, About us, no date,  
http://www.bureauveritas.com/wps/wcm/connect/bv_com/group/home/about-us

http://ec.europa.eu/trade/creating-opportunities/bilateral-relations/statistics/

European Commission, “European Union, Trade in goods with Japan”, no date.  
http://ec.europa.eu/trade/creating-opportunities/bilateral-relations/statistics/

International Electrotechnical Commission, IEC, IEC Members, no date.  


ISO, Profile page for Member Body JISC, no date.  
http://www.iso.org/iso/about/iso_members/iso_member_body.htm?member_id=1835

Japanese Accreditation Board (JAB), Outline, no date.  
http://www.jab.or.jp/en/about/profile/

http://www.jisc.go.jp/eng/

https://www.jisc.go.jp/eng/cooperation/conf_e.html

Japanese International Standards Committee (JISC), JIS mark, no date.  
http://www.jisc.go.jp/eng/jis-mark/newjis-eng.html

http://es.slideshare.net/natsu214/japanese-industrial-standard

http://www.jisc.go.jp/eng/wto-tbt/


D2.2: Consolidated report on security standards and certification

CRISP project


5. INTERNATIONAL STANDARDISATION ACTIVITIES

5.1. INTRODUCTION

This chapter provides an overview of international security standardisation activities. International standardisation is facilitated by the ISO and the IEC. IEC is responsible for all standardisation activities in the field of electrotechnics, IT and ICT. All other sectors are covered by ISO. The standards are jointly developed in technical committees (TCs) by experts from all over the world, representing national points of view. These TCs report to the ISO Technical Management Board, which is the governing council of ISO.

On a global level, many standardisation activities take place in all different kinds of sectors, covering products, systems, services and management systems. A special group of standards are the conformity assessment standards. These standards describe the requirements set of certification institutes, according to which they can get accredited by an accreditation body.

Security standards are developed in several TCs. Some of them have a specific focus on security, other develop standards relevant for security, even though their main focus is not on security. This chapter describes the security related standardisation activities carried out within the main ISO and IEC TCs.

5.2. OVERVIEW OF TECHNICAL COMMITTEES

As described above, many TCs develop standards related directly or indirectly to security. Often, security is one of the issues addressed in a standard. Below is a list of the main international TCs, developing standards with a focus on security:

- ISO/TC 68 Financial services
- ISO/TC 85 Nuclear Energy
- ISO/TC 92 Fire safety
- ISO/TC 94 Personal safety
- ISO/TC 207 Environmental management
- ISO/TC 224 Service activities relating to drinking water supply systems and wastewater systems - Quality criteria of the service and performance indicators
- ISO/TC 262 Risk Management
- ISO/TC 292 Security
- ISO/IEC JTC 1/SC 17 Card and personal identification
- ISO/IEC JTC 1/SC 27 IT Security techniques
- ISO/IEC JTC 1/SC 31 Automatic identification and data capture techniques

---

5.3. **WORK OF SPECIFIC TECHNICAL COMMITTEES**

**ISO/TC 68 Financial services**

ISO TC 68 (TC 68) is the ISO committee primarily designated to develop standards and technical reports for the financial services businesses and their transactions.\(^{841}\) The Business Plan of the TC describes its activities as follows:

"Financial services include depository institutions (which traditionally are recognized as financial institutions), non-depository institutions (or finance companies), consumer and commercial lenders that raise funds in the capital markets, the buy and sell side of the securities markets, private equity firms, mutual fund complexes, central banks, electronic clearing networks and other financial intermediaries, as well as mortgage and insurance companies. Originally formed in 1948, TC 68’s work continues to grow and two of the main evolving areas in this TC are related to cross-border processes and the needs for information security."

The work under ISO/TC 68 is carried out within multiple subcommittees. The main subcommittee working on security-related issues is SC 2 which focusses on information security for the financial sector. Two specific areas SC 2 focusses on are data security and data privacy. Within ISO/TC 68, the development of standards for data security and data privacy are considered to be assisting financial institutions in defining controls to protect customers' sensitive personal information, which can be a very important addition to legislative and regulatory activities aiming at responding to the increasing number of security breaches.

The availability of personally identifiable information facilitates the commission of fraud in other channels such as telephone banking. Decreased opportunities for fraudsters to gain access to account information in online transaction channels is a result of the introduction of strong authentication. This has seen an increased focus on Call Centre vulnerabilities for fraudulent transactions, where identity proofing is often done through the verification of personal information such as date of birth and mother’s maiden name. All these measures are based on standards developed within ISO/TC 68. The following figure summarises the work of the TC. Based on the current work of the committee, almost no link to security certification could be identified.

http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commitid=49650

\(^{842}\) ISO/TC 68, op. cit., no date, p. 1
Most important security-related standards of the TC | ISO 20022 Universal Financial Industry Message Scheme  
ISO 17442 Legal Entity Identifier (LEI)  
ISO 9564-1 Personal Identification Number (PIN), principles and requirements

Security-related standards of the TC which form the basis of testing and certification processes | None

CABs that are responsible for issuing such certificates | No answer

What is standardised: products, component, material, processes, procedures, system or service | Products, services, processes, procedures, systems

Security-related standards which are related to European directives or regulations | None

Major topics of the security-related standards including beyond security, such as trust, efficiency and freedom infringement | Privacy is an important issue in standards related to financial services.

Main effects on the market so far | General acceptance of the use of PIN and PEI.

Additional security-related standards of the TC that might form the basis of testing and certification processes | None

CABs that might be responsible for issuing such certificates | No response

Source: ISO experts
Figure 111: Overview of the activities of ISO TC 68

ISO/TC 85 Nuclear Energy

The objectives of ISO/TC 85 are to improve efficiency, safety and radiological protection for all nuclear activities, nuclear technologies and applications of ionising radiation, and sustain the present globalization of the markets with new international standards. The committee develops standards regarding nuclear energy, nuclear technologies and radiological protection. They include measurement standards, standards specifying material and equipment, system specifications and management systems and conformity assessment.

ISO/TC 85 SC 2 focuses on the protection of individuals (workers, patients, members of the public) and the environment against all sources of ionising radiations in planned, existing or emergency exposure situations. These situations can be linked to nuclear, industrial, medical and research activities. At the time of writing this report, an internal discussion is taking place within ISO/TC 85, to decide on the need for standards in support of radiological diagnosis in crisis situations (airborne measurements, statistics for soil or food sampling).

---

http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commitid=50266
Most important security-related standards of the TC | ISO 12749 Nuclear energy, nuclear technologies, and radiological protection -- Vocabulary
--- | ---
Security-related standards of the TC which form the basis of testing and certification processes | None
CABs that are responsible for issuing such certificates | None
What is standardised: products, component, material, processes, procedures, system or service | Procedures, materials, products
Security-related standards which are related to European directives or regulations | None
Major topics of the security-related standards including beyond security, such as trust, efficiency and freedom infringement | None
Main effects on the market so far | Unknown
Additional security-related standards of the TC that might form the basis of testing and certification processes | Adapted standards for management systems and conformity assessment, specifically for nuclear sector.
CABs that might be responsible for issuing such certificates | No answer

Source: ISO experts
Figure 112: Overview of the activities of ISO TC 85

Starting in 2008, an ad hoc group under TC 85 focusses on management systems and conformity assessment. This group analysed the nuclear energy industry practices and needs in the field of management systems and conformity assessment. It concluded that on the one hand, nuclear operators are encouraged and motivated to implement management system standards, but on the other hand, the existing management system standards (ISO 9001, ISO 14001) need some adjustments for them to be fully applicable to the nuclear sector. The ad hoc group advised TC 85 to develop additional requirements to ISO 17000 (certification and conformity assessment), as well as ISO 9001 (management systems). At the time of writing this report, no decision has been taken yet on the adaption of the standards mentioned.

**ISO/TC 92 Fire Safety**

ISO/TC 92 is a horizontal committee, addressing all aspects of fire safety not specifically within the scopes of other TCs. ISO/TC 92 standards are used for the assessment and control of fire risk of materials, products and structures in the broadest sense. The main stakeholders are industry, in particular the construction industry, national and international regulators, consumer groups, research and testing organisations, fire safety practitioners and certification institutes. The following figure summarises the activities of ISO/TC 92.
### Most important security-related standards of the TC

ISO 12828-1 Validation method for fire gas analysis -- Part 1: Limits of detection and quantification  
ISO 13571 Life-threatening components of fire -- Guidelines for the estimation of time to compromised tenability in fires  
ISO 19703 Generation and analysis of toxic gases in fire -- Calculation of species yields, equivalence ratios and combustion efficiency

### Security-related standards of the TC which form the basis of testing and certification processes

ISO 12828-1 Validation method for fire gas analysis -- Part 1: Limits of detection and quantification  
ISO 19703 Generation and analysis of toxic gases in fire -- Calculation of species yields, equivalence ratios and combustion efficiency

### CABs that are responsible for issuing such certificates

Unknown

### What is standardised: products, component, material, processes, procedures, system or service

Processes, procedures, components, materials

### Security-related standards which are related to European directives or regulations

None, the directives do refer to EN standards.

### Major topics of the security-related standards including beyond security, such as trust, efficiency and freedom infringement

None

### Main effects on the market so far

Unknown

### Additional security-related standards of the TC that might form the basis of testing and certification processes

Unknown

### CABs that might be responsible for issuing such certificates

Unknown

Source: ISO experts

Figure 113: Overview of the activities of ISO TC 92

The main domains for which standards are developed in ISO/TC 92 are:\(^{844}\)

1. Fire safety engineering, design and evaluation methods used to verify that selected fire safety objectives are achieved and to support fire safety management. This includes risk reduction to people, property and the environment.
2. The performance under fire conditions of materials, products, elements of structure, structures and systems and their contents, where appropriate in end-use conditions.
3. Characterisation of occupant performance and behaviour when subjected to fire conditions and fire like emergency situations.

---

http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=50492

Page 391 of 542
Some of the standards developed in ISO/TC 92 are used for certification purposes. They include standards for products and materials, as well as procedures. Fire safety depends, among others, on design, (building) materials, products and fire safety. For all these aspects, standards are developed. They state the requirements, but also the test and validation methods to ensure that the requirements are met. These validation method standards are used for certification.

ISO/TC 94 Personal Safety

ISO TC 94 has the task of standardising the quality and performance of clothing and personal equipment designed to safeguard people against hazards other than those concerned with nuclear radiation. Many countries have put in place legislation to make the workplace safer and the key objective of TC 94 is to provide standards which ensure that products placed on the market provide the level of protection needed to meet the needs of employers and employees and thus help to safeguard the user of personal protective equipment.

ISO/TC 94 develops standards for head, foot, eye, hearing protection, protection against falls, fire-fighters’ equipment and respiratory devices. In the future, the TC will most probably also develop ensemble standards, which are standards regarding the combined use of PPE products.

In Europe, all PPE products have to comply with the PPE Directive. The Directive refers to European standards, in which the requirements for PPE products are written down. Some of these European standards are originally ISO standards, developed in ISO/TC 94, which have been adopted as EN-ISO. The following figure highlights key activities of the TC.

---

845 Personal Protective Equipment
Most important security-related standards of the TC

ISO 3873 Industrial safety helmets
ISO 4007 Personal protective equipment – Eye and face protection – Vocabulary
Personal eye-protectors – Specifications

Security-related standards of the TC which form the basis of testing and certification processes

Nearly all standards containing requirements are used for certification. A list of all standards under TC 94 is available at the ISO website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=50580&published=on&include=true

CABs that are responsible for issuing such certificates

SGS, TÜV, KIWA, BSI, Intertek, and many others

What is standardised: products, component, material, processes, procedures, system or service

Products, procedures

Security-related standards which are related to European directives or regulations

The PPE-directive refers among others to the following standards (all safety-related, not security):
EN-ISO 12402 – floating materials
EN-ISO 4869 – Acoustics – hearing protection
EN-ISO 6529, EN-ISO 6530, EN-ISO 6942, EN-ISO 9185 – Protective clothing

Major topics of the security-related standards including beyond security, such as trust, efficiency and freedom infringement

The standards developed in ISOTC 94 do not relate to security, but to safety. They are about products used on people, meant to keep that person safe.

Main effects on the market so far

Harmonisation of the requirements and testing methods used, confidence in the quality of the products.

Additional security-related standards of the TC that might form the basis of testing and certification processes

No answer

CABs that might be responsible for issuing such certificates

No answer

Source: ISO experts
Figure 114: Overview of the activities of ISO TC 94

According to the figure above, in depth-analyses unveiled that the TC focusses on safety aspects while security is not included in its current scope.

ISO/TC 207 Environmental management

The view of ISO/TC 207 is that environmental management should be an integral part of management systems. Environment is considered to be equally important as quality, risk, security and health and safety. ISO/TC 207 develops standards for among others environmental auditing and performance evaluation, product labelling and declarations, lifecycle assessment, greenhouse gas emission reporting.
The main product of ISO/TC 207 is ISO 14001 Environmental management systems – Requirements with guidance for use. This standard specifies requirements for an environmental management system to enable an organisation to develop and implement a policy and objectives which take into account legal requirements and other requirements to which the organisation subscribes, and information about significant environmental aspects. It applies to those environmental aspects that the organisation identifies as those which it can control and those which it can influence. ISO 14001 is widely used for certification purposes, often in combination with ISO 9001 for quality management.

| Most important security-related standards of the TC | ISO 14001 Environmental management systems – Requirements with guidance for use |
| Security-related standards of the TC which form the basis of testing and certification processes | ISO 14001 Environmental management systems – Requirements with guidance for use |
| CABs that are responsible for issuing such certificates | Many, e.g. DHV, Lloyds, Veritas, BSI |
| What is standardised: products, component, material, processes, procedures, system or service | (management) systems |
| Security-related standards which are related to European directives or regulations | None |
| Major topics of the security-related standards including beyond security, such as trust, efficiency and freedom infringement | Trust can be considered an important issue, when related to the trust people have in the functioning and capacities of an organisation. Communicating the fact that the organisation implemented ISO 14001, may increase the trust other organisations or individuals have in the organisation’s environmental management. |
| Main effects on the market so far | Awareness of the importance of environmental management and insight in this. |
| Additional security-related standards of the TC that might form the basis of testing and certification processes | None |
| CABs that might be responsible for issuing such certificates | None |

Source: ISO experts

Figure 115: Overview of the activities of ISO TC 207

Since the TC could establish a standard that is widely used for certification, it provides an interesting example to learn from its experience.

---

ISO/TC 224 Service activities relating to drinking water supply systems and wastewater systems - Quality criteria of the service and performance indicators

ISO/TC 224, develops standards providing guidelines for service activities relating to drinking water supply systems and wastewater sewerage systems. These standards are designed to help water authorities and their operators to achieve a level of quality that best meets the expectations of consumers and the principles of sustainable development.

<table>
<thead>
<tr>
<th>Most important security-related standards of the TC</th>
<th>Security-related standards of the TC which form the basis of testing and certification processes</th>
<th>The standards are not really related to security and none of the 224 standards are used as a basis for certification as far as known.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CABs that are responsible for issuing such certificates</td>
<td>Not applicable</td>
<td></td>
</tr>
<tr>
<td>What is standardised: products, component, material, processes, procedures, system or service</td>
<td>Terminology and services</td>
<td></td>
</tr>
<tr>
<td>Security-related standards which are related to European directives or regulations</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Major topics of the security-related standards including beyond security, such as trust, efficiency and freedom infringement</td>
<td>Some of the standards describe consumer expectations towards water suppliers. Implementing the standards, will increase the trust of the consumers.</td>
<td></td>
</tr>
<tr>
<td>Main effects on the market so far</td>
<td>No answer</td>
<td></td>
</tr>
<tr>
<td>Additional security-related standards of the TC that might form the basis of testing and certification processes</td>
<td>No answer</td>
<td></td>
</tr>
<tr>
<td>CABs that might be responsible for issuing such certificates</td>
<td>No answer</td>
<td></td>
</tr>
</tbody>
</table>

Source: ISO experts

Figure 116: Overview of the activities of ISO TC 224

According to the figure above, an in depth-analysis showed that the TC is not active in the security field. Since the TC focusses on critical infrastructure and also on services, CRISP’s further work can provide enriching solutions for for the field of interest of the TC.

ISO/TC 262 Risk Management

Management of risk is considered to be an important part of management of organisation, since the acknowledgement of and preparedness towards the occurrence of risk can make the difference between an organisation surviving or not surviving an unexpected situation. The aim of ISO/TC 262 is to develop standards giving guidance on how to implement risk management in an organisation.
The main publications of ISO/TC 262 are:

- ISO Guide 73 – Risk management – Vocabulary
- ISO 31000 – Risk management – principles and guidelines and
- ISO/TR 31004 – Guidance for the implementation of ISO 31000

ISO 31000 is widely used for internal and external risk management auditing, but is not written in such a way that it can be used for certification.

<table>
<thead>
<tr>
<th>Most important security-related standards of the TC</th>
<th>ISO 31000 Risk Management – Principles and guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security-related standards of the TC which form the basis of testing and certification processes</td>
<td>None</td>
</tr>
<tr>
<td>CABs that are responsible for issuing such certificates</td>
<td>None</td>
</tr>
<tr>
<td>What is standardised: products, component, material, processes, procedures, system or service</td>
<td>Management systems</td>
</tr>
<tr>
<td>Security-related standards which are related to European directives or regulations</td>
<td>None</td>
</tr>
</tbody>
</table>
| Major topics of the security-related standards including beyond security, such as trust, efficiency and freedom infringement | Implementing a risk management system (comparable with a quality management system), and proving that it is implemented, has a positive effect on many topics:  
- It increases trust from customers and other related parties  
- Managing risk in a coherent way increases organisational efficiency  
- Dealing with risk, identifying risks timely, and knowing what to do when a risk occurs, increases the security of the organisation. |
| Main effects on the market so far | No answer |
| Additional security-related standards of the TC that might form the basis of testing and certification processes | No answer |
| CABs that might be responsible for issuing such certificates | No answer |

Source: ISO experts
Figure 117: Overview of the activities of ISO TC 262

Although the work of the TC does not include standards used for security-related certification, it has characteristics to learn from. In particular its standard ISO 31000 is an interesting example for a specification that is widely used for conformity assessment.
ISO/TC 292 Security

ISO/TC 292 Security was established on January 1, 2015. Until that date, several TCs developed security standards. To avoid any possible overlap or contradictions in standards being developed and to ensure a more efficient and effective standardisation process, the ISO Technical Management Board (ISO/TMB) decided to combine the following former TC into the newly established ISO/TC 292:

- ISO/TC 8 Ships and marine technology (only the standards on supply chain security)
- ISO/TC 223 Societal security
- ISO/TC 247 Fraud countermeasures and controls
- ISO/PC 284 Private security companies

Bringing the work of all these TCs together, ISO/TC 292 covers a very wide range of security-related standardisation. To ensure that standardisation activities under ISO/TC 292 are carried out in the most efficient way, the work is executed by dedicated working groups. At the time of the writing of this chapter, the working group structure of ISO/TC 292 has not been decided on yet.

ISO/TC 292 develops international standards that aim to increase security, i.e. protection of society, individuals and organisations from and response to incidents, emergencies, and disasters caused by intentional and unintentional human acts, natural hazards, and technical failures. An all-hazards perspective is used covering adaptive, proactive and reactive strategies in all phases before, during and after a disruptive incident.

ISO/TC 292 members include representatives from all types of sectors and organisations, both public and private.

Standardisation activities carried out under ISO/TC 292 include the development of standards and technical specification in the field of:

- Security services
- Security operations
- Investigations
- Security personnel
- Physical security
- Fraud and corruption
- Mass evacuation
- Monitoring of facilities with identified hazards
- Emergency management
- Convergent volunteers
- Organisational resilience
- Competencies

From the perspective of CRISP, the profile of the TC shows much potential for collaboration in the context of the project’s further activities.
### Most important security-related standards of the TC

<table>
<thead>
<tr>
<th>Standards</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 22300 Societal security - vocabulary</td>
<td></td>
</tr>
<tr>
<td>ISO 22301 Business Continuity Management -</td>
<td>Requirements</td>
</tr>
<tr>
<td>requirements</td>
<td></td>
</tr>
</tbody>
</table>

### Security-related standards of the TC which form the basis of testing and certification processes

<table>
<thead>
<tr>
<th>Standards</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 22301 Business Continuity Management -</td>
<td>Requirements</td>
</tr>
<tr>
<td>requirements</td>
<td></td>
</tr>
</tbody>
</table>

### CABs that are responsible for issuing such certificates

<table>
<thead>
<tr>
<th>CABs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSI, Lloyds, DNV, SGS, and many more</td>
<td></td>
</tr>
</tbody>
</table>

### What is standardised: products, component, material, processes, procedures, system or service

<table>
<thead>
<tr>
<th>Products</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processes, procedures, services</td>
<td></td>
</tr>
</tbody>
</table>

### Security-related standards which are related to European directives or regulations

<table>
<thead>
<tr>
<th>Standards</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

### Major topics of the security-related standards including beyond security, such as trust, efficiency and freedom infringement

<table>
<thead>
<tr>
<th>Standards</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Especially standardised ways of working in a crisis situation increases efficiency and effectiveness of first responders and command and control centers a lot, which may lead to decrease of the number of casualties.</td>
<td></td>
</tr>
</tbody>
</table>

### Main effects on the market so far

<table>
<thead>
<tr>
<th>Effects</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No answer</td>
<td></td>
</tr>
</tbody>
</table>

### Additional security-related standards of the TC that might form the basis of testing and certification processes

<table>
<thead>
<tr>
<th>Standards</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

### CABs that might be responsible for issuing such certificates

<table>
<thead>
<tr>
<th>CABs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

Source: ISO experts
Figure 118: Overview of the activities of ISO TC 292

### ISO/IEC JTC 1/SC 17 Card and personal indentification

ISO/IEC JTC 1/SC 17 develops standards for cards and personal identification. These standards describe requirements and procedures regarding passports, identification cards, driver licenses, credit cards, etc.

The work is carried out in several working groups, all working on a specific area:

- WG 1 Physical characteristics and test methods for ID-cards
- WG 3 Identification cards - Machine readable travel documents
- WG 4 Integrated circuit card with contacts
- WG 5 Registration Management Group (RMG)
- WG 8 Integrated circuit cards without contacts
- WG 9 Optical memory cards and devices
- WG 10 Motor vehicle driver licence and related documents
- WG 11 Application of biometrics to cards and personal identification.

The following figure summarises the work of the TC.
### Most important security-related standards of the TC

| ISO/IEC 7064 Information technology -- Security techniques -- Check character systems  
ISO 9798 Information technology -- Security techniques -- Entity authentication and many others |

| Security-related standards of the TC which form the basis of testing and certification processes | None |
| CABs that are responsible for issuing such certificates | Products, procedures, systems |

| Security-related standards which are related to European directives or regulations | None |
| Major topics of the security-related standards including beyond security, such as trust, efficiency and freedom infringement | The standards for personal identification relate to trust and freedom infringement. Privacy and protection of personal information is an important issue in the standards |
| Main effects on the market so far |  |
| Additional security-related standards of the TC that might form the basis of testing and certification processes |  |
| CABs that might be responsible for issuing such certificates |  |

Source: ISO experts

Figure 119: Overview of the activities of ISO/IEC JTC 1/SC 17

**ISO/IEC JTC 1/SC 27 IT Security techniques**

ISO/IEC JTC 1/SC 27 develops standards for IT security techniques, including general methods, techniques and guidelines to address both security and privacy aspects.

The work of this subcommittee includes:

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems (ISMS), security processes, security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security;
- Security evaluation criteria and methodology.
The most important and well-known standards from SC 27 are the ISO 27000-series. ISO 27000, 27001 and 27002 are about Information Security Management Systems and give among others requirements against which organisations can get certified.

| Most important security-related standards of the TC | ISO 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary  
ISO 27001 Information technology – Security techniques – Information security management systems – Requirements  
ISO 27002 Information technology – Security techniques – Code of practice for information security controls |
| Security-related standards of the TC which form the basis of testing and certification processes | ISO 27001 Information technology – Security techniques – Information security management systems – Requirements |
| CABs that are responsible for issuing such certificates | BSI, Dekra |
| What is standardised: products, component, material, processes, procedures, system or service | Management systems, processes and procedures |
| Security-related standards which are related to European directives or regulations | None |
| Major topics of the security-related standards including beyond security, such as trust, efficiency and freedom infringement | The standards regarding IT security are closely linked to privacy infringement. Implementing the standards can decrease the changes of unauthorised access to IT systems. |
| Main effects on the market so far | Widely used standards, confidence in IT security systems |
| Additional security-related standards of the TC that might form the basis of testing and certification processes | |
| CABs that might be responsible for issuing such certificates | |

Source: ISO experts

Figure 120: Overview of the activities of ISO/IEC JTC 1/SC 27

Based on the successful implementation of the ISO 2700X series and its use for security certification, the TC gained interesting experience to learn from.

**ISO/IEC JTC 1/SC 31 Automatic identification and data capture techniques**

The scope of ISO/IEC JTC 1/SC 31 is “Standardization of data formats, data syntax, data structures, data encoding, and technologies for the process of automatic identification and data capture and of associated devices utilized in inter-industry applications and international business interchanges and for mobile applications.

The work is carried out in working groups, focussing on data carrier, data structure, performance, real time location systems, mobile item identification and security and file management.
The main achievements of this SC are the standardised methods for bar codes and QR codes, described in ISO/IEC 15420 and ISO/IEC 18004.

| Most important security-related standards of the TC | ISO/IEC 15420 Information technology – Automatic identification and data capture techniques – EAN/UPC bar code symbology specification  
ISO/IEC 18004 Information technology – Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification |
| Security-related standards of the TC which form the basis of testing and certification processes | None |
| CABs that are responsible for issuing such certificates |  |
| What is standardised: products, component, material, processes, procedures, system or service | Processes, procedures, systems, formats |
| Security-related standards which are related to European directives or regulations | Unknown |
| Major topics of the security-related standards including beyond security, such as trust, efficiency and freedom infringement |  |
| Main effects on the market so far |  |
| Additional security-related standards of the TC that might form the basis of testing and certification processes |  |
| CABs that might be responsible for issuing such certificates |  |

Source: ISO experts  
Figure 121: Overview of the activities of ISO/IEC JTC 1/SC 31

Based on the analyses of the ISO TCs in this chapter, relations to ISO TC 292, which represents the expertise of five key security-related committees, will be most important for CRISP’s further work.
5.4. **STANDARDS RELATED TO SPECIFIC CRISP DIMENSIONS**

Based on CRISP’s specific focus not only on security aspects but also on trust, efficiency and freedom infringements, additional analyses were conducted to identify relevant European and international standards in these fields. According to the following figure, many standards and specifications could be identified related to the freedom infringements dimension, which addresses privacy and data protection issues. The overview builds on analyses of the database Perinorm.

### Fundamental Privacy and data protection issues

- CWA 16113 Personal Data Protection Good Practices
- ISO/IEC 24714-1 Information technology -- Biometrics -- Jurisdictional and societal considerations for commercial applications -- Part 1: General guidance
- ISO/IEC 29100 Information technology - Security techniques - Privacy framework
- ISO/IEC 29003 Identity Proofing
- ISO/IEC 29101 Information technology - Security techniques - Privacy architecture framework
- ISO/IEC 29190 (...) Privacy Capability Assessment Model
- ISO/IEC 29134 (...) Privacy impact assessment – methodology
- ISO/IEC 29151 (...) Code of practice for the protection of personally identifiable information
- ISO/IEC 29191 (...) Requirements on partially anonymous, partially unlinkable authentication
- ISO 22307 ISO 22307 Financial services -- Privacy impact assessment

### Classes of data confidentiality and protection measures

- ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security
- ISO/TS 25237 Health informatics – Pseudonymization

### Privacy protection compliant data transfer

- ISO/TR 21089 Health informatics - Trusted end-to-end information flows

### Privacy protection compliant data lifecycle management

- ISO/IEC 24745 Information technology - Security techniques - Biometric information protection
- ISO/TR 15801 Document management - Information stored electronically - Recommendations for trustworthiness and reliability
- EN 15713 Secure destruction of confidential material. Code of practice

### Privacy by Design

- ISO/IEC 15408 Information technology - Security techniques - Evaluation criteria for IT security
- CWA 16113 Personal Data Protection Good Practices
### Privacy Enhancing Technologies
- CWA 16113 Personal Data Protection Good Practices
- CWA 15263 Analysis of Privacy Protection Technologies, Privacy- Enhancing Technologies (PET), Privacy Management Systems (PMS) and Identity Management systems (IMS), the Drivers thereof and the need for standardization
- ISO/IEC TR 24714-1 Information technology -- Biometrics -- Jurisdictional and societal considerations for commercial applications -- Part 1: General guidance
- ETSI TR 187020 Radio Frequency Identification (RFID) - Coordinated ESO response to Phase 1 of EU Mandate M436

### Non-discrimination in the security context
- ISO/IEC TR 24714-1 Information technology -- Biometrics -- Jurisdictional and societal considerations for commercial applications -- Part 1: General guidance

### Exceptions in the application of Privacy and data protection principles
- ISO/IEC 15944-8 Information technology -- Business Operational View -- Part 8: Identification of privacy protection requirements as external constraints on business transactions
- APEC Privacy Framework, Clause 13

### Data protection and privacy in specific areas and scenarios
- ISO 22311 Societal security -- Video-surveillance -- Export interoperability
- ISO TR 12859 Intelligent transport systems -- System architecture -- Privacy aspects in ITS standards and systems
- IEC 62351 series
- IEC/TS 62351-1 Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues
- IEC/TS 62351-8 Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control

Source: Specified content of Wurster (2014), p. 153f

Figure 122: Selected international and European standards in the area of privacy and data protection

In particular the standards **ISO/IEC 29100, ISO/IEC 15944-8 and the CWA 16113** provide interesting input for CRISP’s further work The standard **ISO/IEC 29100 Information technology -- Security techniques -- Privacy framework** includes, among other things, a chapter called "Privacy policies" and a chapter called "The privacy principles of ISO/IEC 29100," in which eleven privacy principles are presented: Consent and choice, Purpose legitimacy & specification, Collection limitation, Data minimization, Use, retention and disclose limitation, Accuracy and Quality, Openness, transparency, notice, Individual participation and access, Accountability, Information security and Privacy Compliance. Since this standard does not provide specifications for security applications, additional work remains.

Exceptions on the application of privacy and data protection principles are described in the standard **ISO/IEC 15944-8:2012 Information technology -- Business Operational View --**
Part 8: Identification of privacy protection requirements as external constraints on business transactions. In section 5.2 it says:

“Legal requirements for the protection of privacy may contain exceptions in its application. The most common exceptions pertain to national sovereignty and security, law enforcement, public security and health. Exceptions of this type often require access to personal information about a particular individual and tracing of other personal information of the individual (…). Rule 001: Where exceptions to the application of privacy principles exist, they should be limited and proportional to achieve the objectives for which there are exceptions to this, and be brought to public attention or be in accordance with the law.”

Privacy and data protection issues in the context of public security are described in particular in the CWA 16113 Personal Data Protection Good Practices. Its Chapter 4 deals with consent and data access rights regarding the individuals themselves. The rights apply to all types of data, such as written information, photos and video recordings. With regard to ensuring public security three exceptions are described:

“Are there any exceptions to the right of access? Yes. […] The Directive [95/46/EC] set out a small number of circumstances in which their right to see personal records can be limited. This is necessary in order to strike a balance between the rights of the individual and some important needs of civil society, on the other hand. For example, a criminal suspect does not have a right to see the information held about them where that would impede a criminal investigation. […]”

Furthermore, CWA 16113 discusses good practices in the handling of information with personal identifiability and describes reasons that justify the processing of personal data. This also includes the reason ‘Necessity to fulfill a task in the public interest’, which specifies data protection issues in the context of societal security.848

5.5. SUMMARY AND CONCLUSION

Japan views international standardisation activities as critical for achieving further economic recovery and growth, as well as enhancing its competitiveness in global markets. The Japanese Industrial Standards Committee (JISC), responsible for the new and existing Japanese Industrial Standards (JIS), strives to ensure Japanese compatibility with respective international standards via participation in respective ISO/IEC TCs. It is estimated that 40% of JIS standards are currently identical to respective ISO/IEC standards, 57% were modified to some degree, and 3% were deemed non-equivalent or substantially different. An even greater ratio is expected to become identical in due future.

Particularly important in this is the continued technical cooperation between Japanese and EU authorities in the CENELEC, CEN and a bilateral849 EU-Japan CA working group. Since 1996, Japan has held annual information exchange meetings with CENELEC and the two

848 Wurster, S., op. cit., 2014
849 JISC, op. cit., 2013, p. 17
organisations that signed a Memorandum of Understanding (MoU) in 2005.\textsuperscript{850} In November 2012, the fifth information exchange meeting based on the MoU was held concurrently with the JISC-CENELEC information exchange meeting in Brussels, Belgium.\textsuperscript{851} A similar MoU was signed with CEN. In addition, a governmental bilateral EU-Japan Working Group on standards and conformity assessment exists under the EU-Japan Industrial Policy and Industrial Cooperation Dialogue.\textsuperscript{852}

With the aim of improvement of the credibility of Japanese certification schemes, the Ministry of Economy, Trade and Industry (METI) also recently published specific “Guidelines for the Improvement of Management System Certification” and initiated the action plan “Japan Initiative for Reliability Enhancement of Certification (JIREC)” targeted at the accreditation bodies in Japan that was well accepted by regional accreditation organisations. The latest developments follow the Fukushima power plant disaster, which lead to a growing market in nuclear security. Japan’s targeted efforts may lead to new and advanced knowledge, which may specifically enrich international standardisation in this field.

5.6. **REFERENCES**


\textsuperscript{850} JISC, "Bilateral negotiations", no date. https://www.jisc.go.jp/eng/cooperation/conf_e.html

\textsuperscript{851} JISC, op. cit., 2013.

\textsuperscript{852} JISC, op. cit., 2013, p. 13
6. PAN-EUROPEAN CERTIFICATION SCHEMES

6.1. INTRODUCTION

There is a limited number of already established pan-European certification schemes from which lessons could be drawn to compliment the agenda set by CRISP. A useful point of departure is provided by ECORYS whose 2011 report Security Regulation, Conformity Assessment & Certification, includes a detailed overview and a number of examples of what are described as ‘supra-national’ (pan-European) approaches to conformity assessment and certification in the security domain. The examples featured in the ECORYS report are:

- Screening equipment in the aviation sector: ECAC-CEP
- Security alarm systems: CertAlarm
- Privacy for IT products: EuroPriSe
- Video-surveillance in urban areas: Charter for the democratic use of video surveillance (‘code of practice’)

as well as the international initiatives Common Criteria, Open Network Video Interface Forum (ONVIF) and the Physical Security Interoperability Alliance (PSIA).

Whilst these examples are intended to be useful in demonstrating the advantages of harmonised approaches, it is important to take heed of the caveat included by ECORYS. ECORYS caution that in most cases the six approaches outlined are relatively new and “accordingly, their lack of maturity makes it difficult to assess their relative strengths or weaknesses”. Therefore, an updated analysis is necessary now.

Besides a detailed description of these certification schemes, this chapter also presents solutions for remotely piloted aircraft systems, privacy seals and international trade. It describes the CE marking as a successful European approach in general, outlines ideas for an ‘EU security label’ and highlights new European framework conditions which are relevant for further

---

853 It is important to acknowledge that there have been a number of EU supported projects (some completed, others ongoing) that have addressed the issue of conformity assessment, certification and standardisation in the area of security and in the context of the European Union. Examples of such work in the in the area of security that have recently been completed include: BioTesting Europe (Towards a Network for Testing and Certification of Biometric Components and Systems - ftp://ftp.cordis.europa.eu/pub/lp7/security/docs/bio-testing-europe_en.pdf); Staborsec (Standards for Border Security Enhancement - ftp://ftp.cordis.europa.eu/pub/lp7/security/docs/staborsec_en.pdf); and Creatif (Network for Testing Facilities for CBRNE detection equipment – http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item_id=6296&lang=en, pp. 12-13). In addition, a number of collaborative research projects within the European Commission’s Seventh Framework and Horizon 2020 research programmes have worked to signal the importance of standards and certification development as a concomitant to research in order to facilitate development and workability of innovative security and defence solutions. Examples are: COBACORE (COmmunity BAsed COMprehensive Recovery); DESTRIERO (A DEcision Support Tool for Reconstruction and recovery and for the IntEroperability of international Relief units in case Of complex crises situations, including CBRN contamination risks); S-HELP (Securing Health. Emergency. Learning. Planning – Development of Decision Support Tools for Improving Preparedness and Response of Health Services Involved in Emergency Situations); and SECTOR (which addresses the area of a secure European common information space for interoperability of first responders and police authorities).

854 ECORYS, op. cit., 2011.

855 With regard to other sectors covered by the ECORYS study – maritime/ports, urban transport, and other critical infrastructure (e.g. power generation, transmission and diffusion) – most supra-national regulations are pitched in terms of requirements for overall security procedures and processes. ECORYS suggest that typically such regulations do not set out performance or technical requirements for security products.

actions. In addition to these European examples, international certification schemes will be presented in the next chapter.

6.2. **DETECTION SYSTEMS, SECURITY SCANNERS AND SCREENING EQUIPMENT**

The European Civil Aviation Conference (ECAC) is an inter-governmental organisation of 44 Member States that works with various Governmental and non-Governmental civil aviation agencies with the stated mission of the promotion of the continued development of a safe, efficient and sustainable European air transport system. In order to achieve these aims, the ECAC wants to see a shift toward a European, rather than distinctly national, approach to security in the European air transport system. The ECAC wants to “harmonise civil aviation policies and practices amongst its Member States”, and to “promote understanding on policy matters between its Member States and other regions of the world”. The ECAC actively seeks and promotes arrangements, understandings and contacts with other regional organisations and States on a range of civil aviation issues of common interest. With regard to security equipment in civil aviation, the EU regulatory framework identifies acceptable screening methods, including detection systems and security scanners, for passengers and luggage.

The ECAC has established a process for evaluating security equipment, namely the Common Evaluation Process for security equipment (CEP). This process is based on a common methodology for testing security equipment which is developed within the ECAC Technical Task Force. CEP applies to Explosive Detection Systems (EDS), Liquid Explosive Detection System (LEDS), and security scanners. This framework incorporates unified testing methodologies (Common Testing Methodologies, CTM) per type of equipment. As well as testing technical aspects, the CEP also sets out administrative procedures to supply a service to ECAC Member States that delivers what ECORYS describe as “a robust, reliable, repeatable and broadly acceptable basis for national certification”. Figure 12322 shows ECAC’s current accomplishments.

---

857 European Civil Aviation Conference, “European Civil Aviation Conference”, no date, www.ecac-ceac.org
862 Testing is conducted by a limited number of laboratories designated to the CEP by their national Appropriate Authorities. Currently there are only four test centres where EDS can be assessed and three test centres where LEDs can be assessed. Importantly, the accreditation of laboratories are currently not accredited on EU level but merely selected by ECAC. These laboratories do therefore not issue legally binding certifications, but only non-binding test results. Along with performance criteria established under EU regulations, the ECAC has established a Technical Task Force responsible for undertaking the development of technical specifications and testing methodologies to verify compliance with the standards required for deployment in European Airports.
863 ECORYS, op. cit., 2011, p. 158.
864 Weinzierl, op. cit., 2014
Regarding body scanners, the European test procedure ECAC CEP is combined with additional national requirements in the different Member States.\textsuperscript{865}

In order to meet the needs of the future, ECAC comprises several working groups, which work in particular on the six following issues\textsuperscript{866}.

In the field of \textbf{Advanced Cabin Baggage Screening (ACBS)} it works on further specifications regarding the screening of electronic devices and liquids including harmonisation with the U.S. Transportation Security Administration (TSA) and develops conditional test methods (CTM).\textsuperscript{867}

Another area of interest is \textbf{Explosive Trace Detection (ETD)}, in which ECAC currently has two priorities: particle analysis (trace detection) and air analysis (vapor detection). Regarding particle analyses, EU specification 1 - ECAC CTM (2014) was developed, which describes a test methodology (CTM) for the relevant area. Activities in the area of air analyses include the development of EU specifications / test methodologies for object testing including baggage and containers testing. Further efforts have been dedicated to the EU specification for Remote Explosive Scent Tracing (REST) and people screening. The EU specification 1 / ECAC CTM is almost totally harmonized with relevant TSA specifications. Based on its work in the ETD field, ECAC authorized specific test centers in the EU. ECAC’s next steps in the ETD field include the harmonization of the ETD test methodolog with the TSA, work on EU specification 2 ETD and EU specification EVD.\textsuperscript{868}

A specific field of interest is vapor detection. EU specifications to not yet exist in this area but a European working group for the development of the test methodologies has been established. In addition, ECAC participates in several research efforts in the following areas:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Explosive Detection Systems (EDS)</td>
<td>3</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Body scanners (SSc)</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Liquid Explosive Detection Systems (LEDS)</td>
<td>12</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Explosive Trace Detectors</td>
<td>2</td>
<td>12</td>
<td>3</td>
</tr>
</tbody>
</table>

Figure 123: ECAC’s current accomplishments

\textsuperscript{865} Weinzierl, op. cit., 2014
\textsuperscript{866} Weinzierl, op. cit., 2014
\textsuperscript{867} Weinzierl, op. cit., 2014
\textsuperscript{868} Weinzierl, op. cit., 2014
D2.2: Consolidated report on security standards and certification

CRISP project

- Development of sensors capable of detecting explosives in the air (artificial noses)
- Prototype for gas detections
- Development of methods for specified testing of gas detectors for explosives

As mentioned earlier, ECAC also works in the field of Liquid Explosive Detection Systems (LEDS) and develops a proposal for the testing of device combinations. Therefore, Explosive Detection Systems (EDS) in general are another relevant topic of current activities. ECAC works on testing a more flexible test (with greater variety) of explosives. The EU specification 2 on EDS baggage check runs out in 2020/2022. Its successor, EU specification 3 is valid from 2014 onwards while EU specification 4 is already planned. Currently EDS baggage checks concentrate on 2D analyses and 3D EDS (CT-X-Ray) while systems of systems specifications are planned. Additional current issues include specified interfaces as well as an improvement of the picture quality. In addition, ECAC recently established a new test center in Spain.

Other relevant issues include change and configuration management (CCM) for essential parts, routine testing for all control equipment as well as a test methodology for various scanners. In addition, ECAC conducts several research projects to improve the testing of body scanners.

Whilst the overall aim of the ECAC CEP is to provide a harmonised evaluation of different categories of security equipment, there are problems. ECORYS comments that at present the ECAC CEP is only applied to a limited number of categories of equipment and significantly, ‘does not provide a common European-wide certification programme or for direct enforced mutual recognition of equipment certified at a national level’. In addition, the ECAC CEP does provide for conformity assessment (or certification) beyond the aviation sector. Despite efforts towards a common evaluation processes for security equipment, the evaluation does not constitute an approval or certification of the equipment by ECAC. Final approval or certification of equipment remains the responsibility of the Appropriate Authority for aviation security in each ECAC Member State. As a result, there is no complete harmonisation of performance requirements across countries and, consequently, there are differences in national conformity assessment and approval/certification.

869 Weinzierl, op. cit., 2014
870 Weinzierl, op. cit., 2014
871 ECORYS, op. cit., 2011, p. 158.
6.3. **Security Alarm Systems**

Security alarm systems are presented in the ECORYS report in acknowledgment that some European performance standards already exist in this area. CertAlarm was originally initiated by Euralarm, the European Trade Association for electronic and security alarms sector. It is now an independent, not for profit, industry-led certification mechanism.

CertAlarm was officially established in 2010 with the aim of developing and advancing an independent pan-European “one-stop testing and certification” process in the fire protection and security systems industry. Products are tested by independent and accredited laboratories to EN54 fire standards and EN5013X security standards. CertAlarm works through independent, fully accredited, Test Laboratories and Certification Bodies to ensure that:

- Certified products and systems truly meet the exact requirements that are contained in the relevant standards;
- Manufacturers’ production control and Quality Management Systems ensure consistent production standards.\(^{872}\)

Through its members, CertAlarm is able to work with all sections of the industry, users, response authorities and standardisation bodies. CertAlarm states that it develops and improves product standards and methods of assessment to ensure that certified products meet the needs of specifies and users consistently and reliably. It is also interesting to note that CertAlarm actually defines and owns certification schemes.

CertAlarm has been acknowledged by the EA and it is claimed on its website that it represents “the only European Accreditation endorsed certification scheme for the fire and security industry”. Furthermore, CertAlarm suggest that “Our Certification Schemes guarantee compliance to European Product, System, Installation and Service Standards”.\(^{873}\)

Certification is initially available for:

- Intrusion and hold-up alarm system components (using EN50131 series standards), including:
  - Control and indicating equipment
  - Power supplies
  - Detectors
  - Warning devices
- Alarm transmission systems and components (using EN50136 series standards)

CertAlarm offers a “pan-European Mark” and its scheme was developed with the aim of “superseding country-specific certifications”.\(^{874}\) The ‘CertAlarm Quality Mark’ is a Quality Mark applied to certified products or services meeting the requirements of the CertAlarm System:

“The CERTALARM Mark is a third party certification mark, applied voluntarily to a product, system or service after demonstrating compliance with the require-

---

\(^{873}\) CertAlarm, “CertAlarm”, no date, http://www.certalarm.org/ca/content/certalarm
\(^{874}\) CertAlarm “FAQ and European Market”, no date, http://www.certalarm.org/ca/content/faq-and-european-market
ments of the standard(s) specified in “CERTALARM System: Certification Rules - Part 2 - Standards specified for various products, systems and services” and applicable at the time that the product or service is evaluated and certified”. 875

The CertAlarm Quality Mark is designed to ensure that a security product or system is reliable, truly fit for purpose and compliant with the applicable standards and relevant EU directives and regulations. The CertAlarm Quality Mark guarantees compliance with any standard covered by the CertAlarm system today, including all ENs applicable to fire and security systems.

The CertAlarm scheme is now widely accepted across the EU, with many of the leading manufacturers of fire and security products gaining third party certification. CertAlarm also stated that they are committed to improving and extending the scheme. Later extension will include:

- Intrusion and hold-up alarm systems (when standards become available!)
- CCTV systems and components (using EN50132 series standards)
- Access control systems and components (using EN50133 series standards)
- Social alarm systems and components (using EN50134 series standards)
- Alarm systems and components for vehicles and other mobile applications
- Lone worker protection systems. 876

CertAlarm is also working on the “development of pan-European standards to ensure a common integrated solution for mass notification and public alert systems”. 877

ECORYS have suggested that the CertAlarm label could be productively used as a model that could be extended to other security products. 878 However there are issues, as identified in the European Commission Security Industrial Policy Action Plan, the CertAlarm system is faced with the problem that it is privately run and that Member State authorities have no obligation to accept certificates established under the scheme. 879 In addition, as the Commission points out, “authorities of Member States have no obligation to accept certificates established under the CertAlarm scheme”. 880

6.4. REMOTELY PILOTED AIRCRAFT SYSTEMS

This chapter presents multinational certification solutions for civil drones by EASA. At the current stage, the European Aviation Safety Agency (EASA) is competent for drones with a Maximal Take-Off Mass (MTOM) above 150 kg that are not used for the military, customs, police, search and rescue, firefighting, coastguard or similar activities or services and are not specifically designed or modified for research, experimental or scientific purposes to be produced in very limited numbers. More concretely, one section of the General Aviation Department is responsible for the certification of Remotely Piloted Aircraft Systems (RPAS), together with the certification of other aircraft types.

At the moment, RPAS operators are supposed to use EASA policy statement Airworthiness of unmanned aircraft Systems (E.Y013-01) for the certification of drones, which provides guidance to part - 21 subpart B of the Commission Regulation 1702/2003. Authorization of drone operations involving drones with an MTOM of less than 150 kg, in contrast, is to be regulated on a national level. Currently, 11 European countries (Austria, Belgium, Denmark, Finland, France, Germany, Ireland, Italy, Spain, Sweden and the United Kingdom) have rules on drone regulation and 16 countries are developing rules but the processes are not harmonized. Therefore, a comprehensive approach is focused by the institutions involved.

For example in the Riga declaration from 6th March 2015 which brought together the main representatives of the European aviation industry the importance of joint European action in the field of drone regulation was highlighted. This goes even further, stating the need for essential requirements to be harmonized on a global level. Also the need to develop technologies and standards for full integration of drones in the European airspace including the non-segregated airspace was stressed.

Institutions involved

As is clearly apparent from Figure 124123, there is a multitude of actors involved in the harmonization process which all have published certain regulations.

Next to EASA there are EUROCAE and EUROCONTROL operating on the European level. EUROCAE is a European organisation dedicated to the development of technical standards in support of the aviation community. Among its functions, it produces standards used in the certification of avionics and approval of CNS and ATM equipment and applications, provides all aviation stakeholders with a forum to work together to achieve an effective standardisation framework in Europe and offers a proven mechanism for the development of required

---

884 EASA, "RPAS-EASA update", 12.02.2015, p. 3.
886 EUROCAE standards for future aviation, Home, no date. https://www.eurocae.net/
887 communications, navigation, surveillance and air traffic management systems
aviation technical standards and other associated documents. It has over 160 members from countries in Europe and beyond representing all main stakeholder categories. Among the relevant EUROCAE activities, there are two working groups. The working group on UAV Systems (WG-73), created in early 2007, is to deliver technical standards and appropriate guidance material to enable the safe operation of RPAS in all classes of airspace and in all operational environments. The work is to address the differences between RPAS and manned aviation and to deliver appropriate solutions for RPAS, developing recommendations intending to assure the safe, efficient and compatible operation of UAS with other existing airspace users (focus on operations in Airspace Classes A, B and C). The WG-93 (Light Remotely Piloted Aircraft Systems Operations), created in 2012, is tasked to develop standards and recommendations for guidance material for the safe operation of light RPAS, sequenced in order of priority for the community, and primarily directed towards National Aviation Authorities.

EUROCONTROL is the European Organisation for the Safety of Air Navigation, an intergovernmental Organisation with 41 Member States, committed to building, together with its partners, a single European sky that will deliver the air traffic management performance required for the twenty-first century and beyond. Among other activities, they support the European Commission, EASA and National Supervisory Authorities in their regulatory activities.

On an international level, there are the institutions ICAO and JARUS. The International Civil Aviation Organization (ICAO) is a specialized agency by the UN. It works with the Member States and global aviation organisations to develop international Standards and Recommended Practices (SARPs) which states currently reference when developing their legally-enforceable national civil aviation regulations.

The Joint Authorities for Rulemaking on Unmanned Systems (JARUS) are a group of experts from the National Aviation Authorities (NAAs) and regional aviation safety organisations. Currently its secretariat is provided by EUROCONTROL and the Federal Aviation Administration (FAA). Its purpose is to recommend a single set of technical, safety and operational requirements for the certification and safe integration UAS into airspace and at aerodromes (compare JARUS standards). The material will be made available to interested parties such as ICAO, EASA, NAAs and industry, for consideration and use. The objective of JARUS is to provide guidance material aiming to facilitate each authority to write their own requirements and to avoid duplicate efforts.

---

Apart from that, standard bodies come into play. Minimum Operational Performance Standards (MOPS) provide standards for specific equipment, i.e. for all units necessary for the system so it properly performs its intended function. MASPS (Minimum Aviation System Performance Standards) specify characteristics that are useful to designers, installers, manufacturers, service providers and users of systems intended for operational use within a defined airspace.\footnote{Radio Technical Commission for Aeronautics, “Standards & Guidance Materials”, no date. http://www.rtca.org/documents}

**Recent Developments and Outlook**


The EASA is primarily responsible for safety-related issues, while aspects concerning privacy and data protection are still to be dealt with by the national states. One of the core issues of the Concept of Operations is the introduction of three categories of operations and an associated risk-based regulatory regime: Open, Specific and Certified (see Figure 125124). At this, commercial and non-commercial operations shall be treated in the same manner. The current MTOM-based separation of responsibility between the EASA and the national states will then be rendered obsolete.

The new categorization would entail that for operations of the group “open” no airworthiness standards or licenses for operators and pilots will be required. Instead, industry standards shall apply. For the “specific” category operations authorizations will be issued by either National Aviation Authorities (NAAs), probably supported by Quality Entities or by specifically ap-
proved organisations. In the “certified” category multiple certificates like in manned aviation and additional, more specific certificates will be required. For further information, look at the next figure and the concept paper.

Source: EASA, "RPAS-EASA update“, 03/2015, p. 10
Figure 125: Categorisation of drone operations

In June 2013 the European RPAS Steering Group, established by the European Commission, published the roadmap for the integration of civil Remotely-Piloted Aircraft System into the European Aviation System. The roadmap establishes a work programme to achieve full RPAS integration in four timeframes linked to the ICAO Global Air Navigation Plan and the Aviation System Block Upgrades (2013, 2018, 2023 and 2028) with initial priority on harmonization of rules to safely open the internal market for light RPAS (i.e. below 150 kilos operating mass) and parallel extension of scope of EASA, paving the way for common rules to be published soon after 2018. A detailed overview of current developments and actions for the near future in the context of a harmonized approach is presented in the roadmap in Figure 126.
6.5. **PRIVACY SEALS**

Europrise, the European Privacy Seal, is a European scheme providing privacy and data protection certification for Information Technology products and Information Technology-based services. Europrise is described as offering "a trans-European privacy trust mark issued by an independent third party certifying compliance with the European regulations on privacy and data protection". In a recent European Commission report from the EU Privacy seals Project, Europrise is included as representing the only pan-European privacy seal scheme based on EU privacy and data protection law under Directive 95/46/EC and Directive 2002/58/EC.

The European Privacy Seal certifies that an Information Technology product or Information Technology based service is in compliance with European regulations on privacy and data protection, taking into account the legislation in the EU Member States. The European Privacy Seal certifies that a product or service has been checked by independent experts and approved by an impartial privacy organisation. The Europrise value of a trust mark is, according to Europrise, based on the value of its criteria. On its website, Europrise provides a brief...
account of this as follows: “Together with a transparent certification procedure conducted by a financially independent and impartial third party they build the foundation for confidence and trust”. The meaningful criteria are:

- Based on relevant legal requirements to
- Facilitate legal compliance,
- Freely accessible by the public, and
- Verifiable. 899

The Europrise criteria are built on the requirements of the European Data Protection Directive (Directive 95/46/EC) and other relevant EU regulations in relation to data protection, such as the E-Privacy Directive. In their catalogue, Europrise provides a reference to the respective legal article and document the criterion refers to. 900 Europrise claims that their criteria ‘translate’ requirements into questions that can be answered in the context of an audit or certification. According to Europrise, it is the responsibility of the certification body to ensure that in any certification procedure the relevant criteria are applied and that all related questions are answered in a plausible manner, the appropriate granularity, and at a uniform and comparable level.

In its report, ECORYS comments that in view of the limited number of products that have undergone evaluation under the Europrise scheme (the Europrise website indicates that 19 certificates (awarded seals) have been issued) and due to the relative infancy of the scheme, it is difficult to evaluate its performance. 901 ECORYS also notes that at present, there is relatively limited visibility for the Europrise scheme and that recognition is limited. ECORYS warns that if these identified failings persist, the Europrise scheme risks becoming yet another ‘certification’ scheme alongside national and other schemes trying, but largely failing, to provide some form of assessment of the privacy and data-protection characteristics of Information Technology products and services.

6.6. **AUTHORISED ECONOMIC OPERATOR**

The Authorised Economic Operator (AEO) is a joint EU certification programme that serves as an internationally recognised quality mark. 902 The creation of the AEO concept represents one of the main elements of the security amendment of the Community Customs Code (Regulation (EC) 648/2005). 903 The AEO certificate acts as a recognised quality mark that indicates that recipients are secure and that customs controls and procedures are efficient and compliant. Member States can grant the AEO status to any economic operator meeting the following common criteria: customs compliance, appropriate record-keeping, financial solvency and,

---

901 ECORYS, op. cit., 2011, p. 165.
where relevant, appropriate security and safety standards.\textsuperscript{904} AEO status is not mandatory and the certificate is issued by public authorities. The status of authorised economic operator granted by one Member State is recognised by the other Member States and thus is valid in all EU Member States.\textsuperscript{905}

Economic operators can apply for an AEO status either to have easier access to customs simplifications or to be in a more favourable position to comply with the new security requirements. Any legal entity established in the EU that is involved in activities covered by Customs legislation and forming part of the international trade supply chain can apply for AEO status. AEO is primarily understood as representing a commercial decision as it gives quicker access to certain simplified customs procedures. However, it is a scheme that has been designed to increase security as well as to harmonise the customs related operations within the EU and make them more efficient. As Aigner writes, “Customs plays an important role in the fight against cross-border crime and terrorism”,\textsuperscript{906,907} the AEO scheme is seen as a means to enhance security controls so that the EU internal market and international supply chain are protected. There are sets of security requirements that must be met. In the context of the UK, HM Revenue and Customs state that there must be measures in place to protect a business and its supply chain against potential risks, whether human, physical, economic or other:

- comply with legal health and safety requirements
- have had a safety and security assessment
- have appropriately secured external boundaries with documented procedures to control access to their premises
- have measures in place to protect their cargo units and measures to prevent unauthorised access to shipping areas, loading docks and cargo areas
- use procedures to secure the safety of their goods during storage, manufacture and transport
- agree appropriate safety and security measures with their suppliers
- carry out security screening and procedures for prospective employees and contracted parties
- train its staff in security and safety requirements.

The criteria for granting a certificate include an appropriate record of customs compliance, satisfactory management systems that allow appropriate customs controls and proven solvency. Additionally, for security and safety, it includes details of the security and safety standards to be met.

\textsuperscript{904} European Commission, op cit., no date.
\textsuperscript{905} European Commission, “Authorised Economic Operators - Query page”, no date.
\textsuperscript{906} Aigner, Susanne, \textit{Mutual recognition of Authorised Economic Operators and security measures}, World Customs Journal Volume 4, Number 1, 2011, p. 47.
6.7. CE MARKING

The European Union introduced CE marking in 1985 as a system developed in order to promote free trade within the Community. The development of the CE marking system has largely ended the tendency for inconsistent national product requirements. Hanson writes that at the heart of CE marking are “a set of product safety standards and a series of conformity assessment procedures that are used to prove that these standards have been properly implemented”. These EU requirements override national requirements. Defining the role of the CE marking, there are three main points. Firstly, CE marking shows that the manufacturer has checked that these products meet EU safety, health or environmental requirements. Second, the CE marking indicates the conformity of the product with the Union legislation applying to the product and providing for CE marking. And third, the CE marking is affixed on products that will be placed on the EEA and Turkish market, whether they are manufactured in the EEA, in Turkey or in another country, allowing the free movement of products within the European market:

“CE marking is a key indicator of a product’s compliance with EU legislation and enables the free movement of products within the European Market. By affixing the CE marking on a product, a manufacturer is declaring … conformity with all the legal requirements to achieve the CE marking.”

The CE marking is required for many products (those product categories subject to specific directives that provide for CE marking) within the European Economic Area (“EEA”, consisting of the 28 EU Member States, and the EFTA countries Iceland, Liechtenstein and Norway). CE marking is mandatory, but only for those products which are covered by the scope of one or more of the New Approach Directives. The CE marking states that a product is assessed before being placed on the market and meets EU safety, health and environmental protection requirements of the applicable directive(s), or, if stipulated in the directive(s), had it examined by a notified conformity assessment body.

Not all products are required to bear CE marking, only those products that fall within the scope of at least one sectoral directive requiring CE marking. Each Directive has slightly different methods of demonstrating conformity depending on the classification of the product and its intended use. Every Directive has a number of ‘essential requirements’ that the product has to meet before being placed on the market. These are in two parts; Protection requirements and Administrative requirements. The protection requirements relate to the design of

---

910 The European Union introduced a series of measures to simplify the movement of goods throughout the European Union (EU) and the European Free Trade Area (EFTA). Some of these measures are known as New Approach Directives. New Approach Directives provide controls on product design and above all, seek to harmonize product safety requirements across Europe. The directives cover a very wide range of product areas including construction products, personal protective equipment and pressure equipment. Their primary objective is to ensure that the products are well designed, and safe for the user. Throughout Europe, where a New Approach Directive is in force, it is necessary for the manufacturer to CE mark their product. CE marking requirements vary from Directive to Directive, and even within Directives. European Commission, “Guide to the Implementation of Directives Based on New Approach and Global Approach”, http://ec.europa.eu/enterprise/policies/european-standards/links/index_en.htm
the product and can be demonstrated by meeting the requirements of the relevant harmonised standards. The administrative requirements relate to how the product is CE marked. Identifying which directive(s) may be applicable, as there may be more than one, involves reading the scope of each directive to establish which apply to the product. To demonstrate that essential requirements have been met, it is recommended that they are in line with the requirements of an applicable ‘harmonised standard,’ which offer a presumption of conformity to the essential requirements, although the use of standards usually remains voluntary. Harmonised standards can be identified by searching the ‘Official Journal’ on the European Commission’s website, or by visiting the New Approach website.912

6.8. **The ‘EU Security Label’**

In its *Security Industrial Policy Action Plan for an innovative and competitive Security Industry* published in 2012, the European Commission has proposed the possibility of developing and adopting an approach in security, for security solutions and services, similar to CE marking. Their proposal would involve producing an ‘EU Security Label’. The ‘EU Security Label’ would, the Commission recommends, be similar in scope and application to the CE marking used in the field of product safety:913,914

In the future, products certified on the basis of an EU wide certification system could receive an “EU Security Label”, similar to the CE marking used in the field of product safety. As suggested by ESRIF, such a label could act as a ‘seal of quality’ for security products (made and validated in the EU).

Over the last decade, ESRIF has persistently made reference to the need for the establishing of an ‘EU Security Label’, contending that such an innovation is a necessary device in the area of security. However, so far the ‘EU Security Label’ has not been subject to sustained development, or moved beyond the basis for discussion. For ESRIF an ‘EU Security Label’ would be influential and useful to the field of security for a number of reasons.915,916 ESRIF proposes that a ‘European Security Label’ will offer a common reference point for security providers, end-users and legislators and is advisable as a means developing a more competitive European security market. This thinking is reflected by Grasso who writes that security, along with safety, must be embedded into systems and certified with proper labelling: “The Security Label will create the confidence that security products and services meet certain quality and are suitable for the intended use.”917 It is envisioned by ESRIF that the results of an ‘EU Security Label’ will include “creating a coordinated accreditation process for test fa-

cilities and auditors, while encouraging appropriate organisations to apply”.\(^{918}\) ESRIF recommends that an ‘European Security Label’ would work to “promote the harmonised application of security measures and common quality levels as the criteria for market access”\(^{919}\) and “should help nudge standardisation and certification processes toward a harmonised application of security measures and quality as the criteria for market access for security products and services”.\(^{920}\)

The creation of a clearer European identity for these security technologies, utilising schemes such as the proposed ‘EU Security Label’, is seen as positive as it could lead to the development of a possible and recognisable ‘EU brand’ in security. Such efforts to develop and establish a security ‘brand’ of sorts, it is hoped by the European Commission, should contribute to enhancing the global competitiveness of the EU companies in the field of security with regards to their main competitors in the United States and China, addressing growing international competition and recent market evolutions.

ESRIF suggests that in its current state, the market needs basic criteria upon which to base decision making regarding the acquisition and implementation of security products, services and the integration of them both. ESRIF also considers that an instrument is required that can enable the procurers of security products and services to make, and justify choice of purchase, adopting recognised security principles. ESRIF cites a number of additional reasons to support the development of an ‘EU Security Label’. For example, ESRIF believes the ‘EU Security Label’ would act as a catalyst for investment in the EU security industry, provide an answer to the present state of real and perceived security (insecurity) in EU countries, and offer protection from charges of negligence and liability plus assistance in risk management for end user.\(^{921}\)

The importance of effective ‘branding’ and a creating and recognisable ‘identity’ should not be underestimated, in the *New Partnership for Security* conference report, David Fairnie, Director of Global Port Solutions at G4S, is reported as agreeing on the need for a European security label. Fairnie warned that European industry risked being left behind, given that international competitors were already moving ahead with such systems.\(^{922}\) He raised the prospect of common EU public procurement in security and suggested that European industry be given an EU “security label” to encourage standardisation. ESRIF has further analysed the concept of a “Security Label” and recommend that such a scheme would be a positive step for global market competition and in supporting effective regulatory enforcement, as well as working to “stimulate innovative technologies that provide the best value for money in the long term, while ensuring interoperability”.\(^{923}\) In addition, ESRIF has identified several sectors to be included in the proposed ‘EU Security Label’, whereby they believe that such processes could further enhance the confidence of citizens in their security: “by introducing a

compulsory ‘privacy & freedom-compliancy requirement’, the Label would at the same time express respect for European civil liberties”.924,925,926

6.9.  REFERENCES

Aigner, Susanne, Mutual recognition of Authorised Economic Operators and security measures, World Customs Journal Volume 4, Number 1, 2011.


de Brichambaut, Marc Perrin, The Return of the Pan-European Security Question, Turkish Policy Quarterly, Vol. 8, No.1,
http://www.esiweb.org/pdf/esi_turkey_tpq_vol8_no1_marc_brichambaut.pdf

CEN, CEN/TC 391 Business Plan Revision 02, November, 2010,


CEN, COMPASS The World of European Standards, 2010.
http://www.din.de/sixcms_upload/media/2896/CEN_compass.pdf

CertAlarm, “CertAlarm”, no date, http://www.certalarm.org/ca/content/certalarm

CertAlarm, CertAlarm System Certification Rules. PART 1 Definition of procedures and conditions for testing and certification, May, 2013,


https://www.commoncriteriaportal.org


European Civil Aviation Conference, “European Civil Aviation Conference”, no date, www.ecac-ceac.org


7. **INTERNATIONAL CERTIFICATION SCHEMES**

7.1. **INTRODUCTION**

This chapter provides an overview of international security assessment solutions, partly in form of standards, partly in form of legal regulations, frameworks, partnerships or initiatives. The classification of these schemes is loosely based on the classification already used in the security standardisation mandate M/487\(^{927}\) and which was also the basis of the glossary for the CRISP project.\(^{928}\) This means solutions in the areas of security of the citizens (including crime prevention and CBRNE), security of infrastructure (including supply chain & cargo security), security & crisis management and border security\(^{929}\) were analysed.

Within CRISP these solutions provide a good insight into harmonisation processes of security PSS apart from important standardisation organisations although they are only a selection amongst a wide range of solutions. Most of them can be regarded as best practice examples or are market leader in their section, but there are also solutions, which show challenges regarding the successful dissemination of multinational solutions for the assessment of security PSS.

7.2. **SECURITY OF THE CITIZENS – CRIME PREVENTION**

Several standards and frameworks exist, which promote harmonisation for security PSS aiming at crime prevention, like for example CCTV surveillance. Although crime prevention does not only aim at citizens’ security, it is an important part of it. While the first presented solution, the open network video interface forum, has a strong technological focus, aiming at the harmonisation of network communication of security systems, the second one, the International Code of Conduct for Private Security Service Providers, aims at setting common requirements for private security personnel – and covers a large amount of difficulties security personnel might be confronted with upon providing a security service.

7.2.1. **OPEN NETWORK VIDEO INTERFACE FORUM (ONVIF)**

The open network video interface forum (ONVIF) is a forum of network security system manufacturers, focused on the development of standards, which are necessary for the communication between linked security products. The ONVIF standards set the requirements for an interface of network video products. These make sure that products of different brands are interoperable and thus can be used within one security system. Interoperable network video solutions are easier to use, more flexible and cost-effective. The first ONVIF core specification was released in late 2008, with the first security product using the specification being released in 2009.

---

\(^{927}\) European Commission, Programming Mandate addressed to CEN, CENELEC, and ETSI to establish security standards, M/487, Brussels 17.02.2011.


The ONVIF specifications are openly available on the ONVIF website making the usage of these specifications open for all manufacturer – although only ONVIF members have access to a specific testing tool and are allowed to claim the conformance with the ONVIF specifications. The primary aim of these specifications is the standardisation of the network interface of the network video products based on Web Services standards. For example the first core specification (ver. 1.0) of the standard covered the following aspects of network communication:

- “IP configuration
- Device discovery
- Device management
- Media configuration
- Real time viewing
- Event handling
- PTZ control
- Video analytics
- Security.”

**ONVIF Profiles**

Since the first ONVIF core specification was released in 2008, a lot has been improved and the latest specifications do not only cover network video products, but also other network security products. These are categorised into profiles that make it easier to identify compatible network security products and features of interoperability. ONVIF profiles define “a specific and unambiguous set of features that an ONVIF Device shall implement and support, and an ONVIF Client shall use to support that particular functional interoperability with an ONVIF Device that claims conformance to that Profile.”

The profile is constant, thus is not affected by the release of new specifications, which entails that ONVIF Devices with the same profile have to be able to communicate with each other, no matter what specification version they use.

Currently there are three ONVIF profiles in operation and one profile in development

| Profile S | The Profile S applies to devices that send video data over an IP network to a client, including audio and metadata streaming. The client thus needs vice-versa to be able to configure, request and control the data send by the device. |

---

Profile C

Devices with compliance to the ONVIF Profile C are devices, which are part of a physical access control system and thus provide information about the entities and their status of the access control system. This can for example be basic door control.\(^{934}\)

Profile G

Profile G compliant devices are devices that are able to record/store video data on the device itself or through an IP network, as for example IP network cameras. The compliant client can configure and control the video-recording through the network and thus enables a communication with the recording device.\(^{935}\)

Profile Q

The Profile Q aims at addressing the new challenges of the market demand of IP network security products, which is mainly the “out-of-the-box” interoperability. There is a high demand of quick install products, compliant devices are automatically discovered and configured by the client. Typical use cases of the Profile Q would be installation of devices, where the client is launched to discover the available devices and configures the IP-address and the like. Also the identification of the firmware of the devices in order to assess the necessity of firmware updates is handled by this profile.\(^{936}\)

The Profile Q is currently available for review on the ONVIF website, thus amendments are still possible.

Source: Own figure
Figure 127: ONVIF profiles

The ONVIF is an important stakeholder in the standardisation of network video devices and access control systems. On the one hand they set really specific standards with a big focus on the interoperability of the scattered field of network security devices. On the other hand are the members of the ONVIF, with a presence of a large amount of manufactures of network security devices, who comply with the interoperability standards. Amongst the 27 full members are manufacturers like Bosch, Cisco, Honeywell, Samsung, Siemens and Sony, beside 22 contributing and 454 user members. Also the transparency and openness of the forum is a good practice and not often observed in the area of standardisation.

While the ONVIF serves as a big advantage regarding the efficiency and efficacy of security measures, mainly due to the interoperability and easiness to use, other dimensions are not really addressed by the specifications and profiles. Although the interoperability is the main aim of ONVIF, features like the security of the transmission should require increased attention – due to the sensibility of data processed by the devices. ONVIF provides a white paper on security recommendations,\(^{937}\) but a direct implementation of high level security standards would be better.

\(^{936}\) ONVIF, “Profile Q Specification”, Release Candidate, version RC 1.0, December 2014.
### 7.2.2. International Code of Conduct for Private Security Service Providers

The international code of conduct for private security service providers (ICoC) is an initiative introduced by the Swiss government, setting standards for private security services, improving the oversight and accountability, and is built on international human rights law. The basis for the code was mainly the *Montreux Document On Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies During Armed Conflict*, as well as the “Protect, Respect and Remedy” Framework and Guiding Principles developed by the Special Representative of the United Nations Secretary-General on Business and Human Rights.

The private security services providers committing to this international code guarantee their respect to the human rights of all person affected by their activities and also guarantee to respect the cultural differences encountered in their activities. This includes not only the population or visitors of a certain area, but also the personnel, the clients and the suppliers of the area of work.

The code covers several principles of human rights with which private security service providers might be confronted, including.\(^{938}\)

<table>
<thead>
<tr>
<th>General Conduct</th>
<th>Security service providers guarantee that their employees respect every person’s dignity and privacy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules for the Use of Force</td>
<td>This means that personnel of private security service providers will not only comply with legal regulations regarding the usage of force, but will also try the avoidance of force by any means and if the usage is necessary, it should be proportionate the situation. The usage of fire arms should also not only comply to national legal regulations, but also only be used in severe necessary cases, like e.g. in self-defence or other persons in case of danger of threat of death.</td>
</tr>
<tr>
<td>Detention</td>
<td>Detention, as well as the transportation or interrogation of detainees should only be carried out by private security service providers if they have a specific contract with the contracting state for detention and their personnel is specifically trained for the handling of detainees. Of course all the other principles of the code apply to detainees as well.</td>
</tr>
<tr>
<td>Apprehending Persons</td>
<td>Similar to the previous principle, it is also important that security service providers do not arrest persons, other than in case of immediate danger for themselves or others, but also for the protecting property. In case of such apprehension, the person should be submitted to a law enforcement authority at the earliest possible moment. Also here the other principles of the code – the respect of human rights – apply to the apprehended persons.</td>
</tr>
</tbody>
</table>

| **Prohibition of Torture or Other Cruel, Inhuman or Degrading Treatment or Punishment** | The prohibition of torture requires that all personnel of private security service providers do not engage in torture, under any circumstances – “contractual obligations, superior orders or exceptional circumstances such as an armed conflict or an imminent armed conflict (...) can never be a justification for engaging in torture.”939 Any act of torture must be reported to the contractor and the national authority of the country of activity. |
| **Sexual Exploitation and Abuse or Gender-Based Violence** | The personnel of the private security service providers will not benefit from or contribute to any form of sexual exploitation (e.g. rape, sexual abuse, harassment, but also prostitution) within the company as well as externally. Any form of sexual exploitation has to be reported to the responsible authority. |
| **Human Trafficking** | Human trafficking is “the recruitment, harbouring, transportation, provision, or obtaining of a person for (1) a commercial sex act induced by force, fraud, or coercion, or in which the person induced to perform such an act has not attained 18 years of age; or (2) labour or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, debt bondage, or slavery.”940 Private security service providers should not only not engage in human trafficking, but also remain vigilant for any forms of human trafficking and report any activity to local authorities. |
| **Prohibition of Slavery and Forced Labour** | Service providers do not engage in slavery or forced labour. |
| **Prohibition on the Worst Forms of Child Labour** | Service providers respect the rights of children and make sure that they are protected from the worst forms of child labour which are slavery, child prostitution or pornography, illicit activities like drug production or trafficking, as well as work which could harm the safety, morality or health of the child. |
| **Discrimination** | The personnel of the private security service providers, as well as the company itself, will not discriminate anyone on the basis “of race, colour, sex, religion, social origin, social status, indigenous status, disability, or sexual orientation.”941 |
| **Identification and Registering** | The provider needs to make sure that every person carrying out the activities is identifiable. The same goes for the vehicles and hazardous material in use. |

Source: Own figure
Figure 128: ICoC principles

Further commitments set by the code imply mainly managing issues but also safety and health issues in the working environment, or the reporting of incidents. These commitments are although only covered in general and do not go into detail concerning specific tasks and duties. It is clearly visible that these principles heavily rely on the human rights, setting reliable standards regarding the conduct of security service providers and their personnel. This is per se not a bad thing, but due to the wide scope of the human rights, specific codes of conducts for definite security services are not covered here (and not possible to be covered) and should therefore be addressed and implemented by other standards.

The International Code of Conduct for Private Security Providers Association was agreed on in February 2013 in Montreux of the governance and oversight mechanism to the ICoC. On the 1 of September 2013, 708 private security service providers had signed the international code of conduct.

7.3. **Security of the Citizens – Privacy**

Another aspect of the security of the citizens that needs to be considered is the area of privacy safeguarding. This is necessary with regard to the other areas of security, as security measures taken there often have a more or less large impact on the privacy of citizens. Furthermore privacy is also an important aspect of the CRISP project – within the STEFi model, which is one of the core concepts of the project, the freedom infringement dimension (and thus also the privacy dimension) of security products, systems and services needs to be assessed for the effective functioning of the relevant solutions.

Although the respect of individuals privacy is dealt with in some of the security assessment solutions presented here (the ICoC for example addresses privacy in the general conduct commitment of private security service providers), it is important to highlight specific privacy related schemes here – as they try contribute in maintaining privacy rights challenged by security PSS.

The European Privacy Seal (EuroPriSe) is a certification for IT products and IT based services, which assesses the compliance of the product or the service with the European data protection regulations in the form of a European privacy certificate. The aim of EuroPriSe is to enhance and ensure privacy through the technology itself, which is the concept of privacy by design. With an enhancement of privacy of IT products and services, the trust of citizens and businesses in these products should improve. In a recent European Commission report from the EU Privacy seals Project, EuroPriSe is included as representing the only pan-European privacy seal scheme based on EU privacy and data protection law under Directive 95/46/EC and Directive 2002/58/EC.

The EuroPriSe is – like other certifications – a way for manufacturers or service providers to demonstrate excellent data protection principles. The EuroPriSe value of a trust mark is, according to EuroPriSe, based on the value of its criteria. On its website, a brief account of this is provided as follows: “Together with a transparent certification procedure conducted by a

---

942 An extensive analysis of the STEFi model and the dimensions (security, trust, efficiency and freedom infringement) is part of the Work Package 4 of the CRISP project.

financially independent and impartial third party they build the foundation for confidence and trust.” The meaningful criteria are:

- Based on relevant legal requirements to
- Facilitate legal compliance,
- Freely accessible by the public, and
- Verifiable.\(^944\)

While the criteria of EuroPriSe highlight the value and importance of the seal, the scheme also addresses the criteria IT products and services should comply with regarding privacy. These criteria are compiled into four sets, of which each contains relevant questions, addressing issues of privacy and data protection.

**Set 1: Overview on fundamental issues**

This first set is necessary to provide an overview of relevant privacy issues relating to the IT product or service and analyses the purpose of the processing operation:

- what personal data is processed and in which categories,
- who is the data controller, and
- whether the data is shared to countries outside the EU and EEA.

Other aspects of the fundamental issues analyse data avoidance and minimisation – thus if personal data collection, processing and sharing is reduced to a strictly necessary minimum and also deleted again after a certain necessary time.

Furthermore, transparency aspects of the data collection and processing are evaluated, assessing whether the users of the IT product or service are informed about the personal data collection, as well as on the description of the product itself in a clear form. The transparency aspect also includes the privacy statement of websites, which should be informative and comprehensible, stating what personal data is processed, who the data controller is, but also where the privacy statement is located and how it’s highlighted.

**Set 2: Legitimacy of data processing**

The legitimacy of the data processing checks whether the operated data processing is in compliance with legal requirements, mainly the European data protection directive\(^945\) and the European directive on privacy and electronic communications.\(^946\) This entails on what legal basis the processing of personal data relies on and if the requirements for the basis are met (on the basis of consent, a contract, a legal obligation, etc.), which is especially important for the processing of sensitive personal data. Furthermore the EuroPriSe criteria on the legitimacy of data processing set requirements for the different phases of the data processing, thus the collection of data, disclosure of data internally and externally, as well as erasure of the data.


(which overlaps partly with the first set of criteria). Other aspects cover the proportionality of the processing, the quality of the data, but also if data is processed by a processor, if automated decision is involved in the processing, as well as regarding the notification and the registration of the data processing.

In regard to the directive on privacy and electronic communications, special restriction on the processing of location and traffic data of electronic communication services are evaluated, including the usage of cookies as well as making unsolicited direct marketing contacts with the users.

**Set 3: Technical-Organisational Measures**

Technical-organisational measures for the protection of the data subject encompass a large amount procedures and techniques in order to grant the security of the processed personal data. This includes the prevention of unauthorised access through measures of access control and access restriction (physical access control, access control to removable storage media, access control to data and programmes, identification and authorisation measures, requirements for passwords). Other mechanisms to guarantee the security of the personal data are through logging mechanisms, which make it possible to track the reading, manipulating or deleting of personal data.

Furthermore a range of technical measures should be implemented on the side of the data processor in order to grant the security of the processed personal data. This includes back-up and recovery mechanisms and mechanisms to prevent accidental loss of data. Also security management increases the safety of the personal data and should therefore be assessed, mainly security policies and risk analysis. But also other measures can be included in the security management section, like for example documentation of data protection measures, or the organisation of data protection and/or security officers.

Lastly this set of criteria also entails specific technical measures, like the encryption mechanisms of the data when they are transmitted or stored on mobile devices. Similar for anonymisation and pseudonymisation, where the effective implementation should be evaluated.

**Set 4: Data subject rights**

The last set of criteria handles the rights of the data subject, again closely related to the European data protection directive. Data subject rights are on the one hand the right to be informed about the data processing, but also about the identity of the data controller, the purpose of the processing, as well as the other rights he or she has regarding the personal data. On the other hand, the data subject has the right of access to data which can be achieved through subject access request addressed at the data controller. The data subject should be granted access to all data on him or her, but also on the purpose of the processing and details of the processing process as well as on the logical structure of the database. The EuroPriSe criteria also analyse how the identity of the data subject is checked upon access request and how the process of the subject access request is handled.

Hand in hand with the right of access to data goes the right of correction and right of erasure of personal data, as they require the right of access beforehand. Here, the criteria are meant to evaluate how these rights are granted and accomplished. Lastly under the data protection directive, the data subject should also have the right of objection to processing, where here again it is assessed how this right is carried out by the data controller.
Beside the rights under the data protection directive, are also the data subject rights under the directive on privacy and electronic communications. These include mainly the right to be informed of personal data breaches, as well as the right to be informed of security risks. Here the EuroPriSe analysis how these rights are adhered by the service operator. Furthermore the directive foresees users the right to confidentiality of the communications which rely closely to the security of the transportation of the personal data – the criteria thus check on the measures preventing tapping and intercepting of communication data.

All in all, EuroPriSe can be seen as a good way for evaluating IT products and services regarding their compliance to the European data protection directive and the European directive on privacy and electronic communications – as those two seem to be the basis for the evaluation criteria. Although both directives are fundamental for privacy rights in Europe, especially the data protection directive is outdated in some instances already (a new directive is currently being negotiated), which thus could also influence the EuroPriSe evaluation of IT products and services. Still, the European privacy seal is a good initiative to promote privacy amongst IT manufacturers and IT-based service providers, as well as trust amongst citizens towards these IT products and services.

Unfortunately, the success of the European privacy seal is only limited so far, from their first seal in 2008 only 21 other seals were issued until 2013. ECORYS also notes that at present, there is relatively limited visibility for the EuroPriSe scheme and that recognition is limited. ECORYS warn that if these identified failings persist, the EuroPriSe scheme risks becoming yet another ‘certification’ scheme alongside national and other schemes trying, but largely failing, to provide some form of assessment of the privacy and data-protection characteristics of Information Technology products and services.

This is an important aspect for the CRISP project, as it shows the difficulties with which ‘unconventional’ security certification schemes have to deal with – with the implementation of privacy aspects, but also like by including trust and efficiency aspects of the security PPS. The EuroPriSe as a very good example of trying to certify data protection aspects in security products and services, can similarly be seen as a good example of the difficulties such schemes have to establish on the market of security certification schemes.

### 7.4. Security of the Citizens / Security of the Infrastructure – Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE)

Threats including CBRNE cover here two kinds of threats, which is why international security assessment solutions of CBRNE are labelled not only as security of the citizens but also as security of the infrastructure. On one hand CBRNE incidents have a wide impact on citizens, often not only of a certain area but more often of larger regions and continents. Security measures and emergency preparedness also go hand in hand here, and need to be specially tailored for the challenges of large scale events. On the other hand, CBRNE facilities as an infrastructure need special security measures, as they are very vulnerable to threats of all kinds, from natural disasters to terrorist attacks. They also cannot really be considered separately as the security of CBRNE infrastructure is – again due to its large scale in case of security breaches – also a matter of security of the citizens.

---

The main focus here will be on the work of the International Atomic Energy Agency (IAEA), which has developed a large amount of security recommendations, covering the wide amount of threats and consequences in the radiological and nuclear area. Beside the IAEA security recommendations, other good practice examples are the CREATIF project – which was already the topic of CRISP’s deliverable 2.1 on security standards and certifications in Europe – and the National Strategy for CBRNE standards in the USA, which is discussed in the respective country report.

### 7.4.1. CREATIF Project

The CREATIF project was funded by the seventh Framework Program and consisted of a consortium of testing facilities for CBRNE detection. The aim of the project was to create a harmonisation within CBRNE detection testing facilities, defining minimum requirements and generating certification strategies. General requirements and finding, as well as specific requirements for each of the fields of chemical, biological, radiation and nuclear, and explosives detection were evaluated.

In summary the main findings of the CREATIF project were that there is a lack of harmonisation of CBRNE test approaches, as there is apparently a reluctance at the testing institutions in sharing their know-how. Ideally, test protocols should be harmonised and a mutual recognition of tests should be targeted.

### 7.4.2. IAEA Nuclear Security Series

In the area of CBRNE security assessment solutions, the international atomic energy agency (IAEA) is one of the main organisations promoting solutions for radioactive and nuclear security threats. We will thus present you here an overview of the recommendations and activities of the IAEA, which should be seen as a summary of the work of the IAEA.

The IAEA Nuclear Security Series is a series of publication of the department of nuclear safety and security of the IAEA, addressing different aspects of nuclear and radioactive security threats, including the prevention, detection and response of theft, sabotage and other malicious acts regarding nuclear and radioactive substances. The drafting of the recommendations is done by the IAEA Secretariat, but also include the assistance of experts from Member and the Nuclear Security Guidance Committee (NSGC).

The nuclear security series is mainly directed at national governments and states for the implementation and strengthening of nuclear security programmes. International security conventions like the UN International Convention for the Suppression of Acts of Nuclear Terrorism, or the Code of Conduct on the Safety and Security of Radioactive Sources relate closely and are complementary to the IAEA publications on security.

---

948 The CREATIF Project was already discussed in the CRISP Deliverable 2.1, and will thus only be mentioned here and not further elaborated. More information available at: Wurster, Simone, Tim Pohlmann, Patrick Murphy, Florian Fritz, Roger von Laufenberg, Jolien van Zetten, Cristina Pauner, Artemi Rallo, Rosario García Mahamut, Rosamunde van Brakel, Alessia Tanas, “Report on security standards and certification in Europe – A historical/evolutionary perspective”, D2.1 CRISP Project, 30. August 2014, p. 120.

The series issues publications in four different categories, nuclear security fundamentals which form the basis of a State’s nuclear security program; nuclear security recommendations which are additional measures States should include in their nuclear security programme to increase their efficacy; implementing guides for the security recommendations; and technical guidance which are supplementary to the implementing guides and address specific technical implementation questions.

**Nuclear security fundamentals publications:**

In the security fundamentals category, the IAEA has released one publication promoting the objective and essential elements on which a State should invest in their nuclear security regime, in order to grant a minimum protection against nuclear threats – the *Objective and Essential Elements of a State’s Nuclear Security Regime*.

The aim of every nuclear security regime should be to protect persons, infrastructure, society and the environment from the consequences of a nuclear threat. Twelve essential elements for a state’s nuclear security regime are recommended by the IAEA:

1. State responsibility to implement and sustain a nuclear security regime.
2. Identification and definition of nuclear security responsibilities of authorities within a state.
3. Legislative and regulatory framework, setting the legal requirements in order to assign authorities and bodies to the responsibilities of the nuclear security regime, including the import and export of nuclear/radioactive material and the detection, deterrent and prevention of illicit trafficking of material.
4. Protection of the international transport of nuclear and radioactive materials.
5. Defining offences and penalties that address illicit acts involving nuclear and radioactive materials, including regulating the prosecution of the acts.
6. Providing an effective international cooperation and assistances with others states and the IAEA, covering the above mentioned elements.
7. Ensuring the identification and assessment of internal and external nuclear security threats.
8. Ensuring the identification and assessment of the potential targets of the threats and the consequences if the targets were to be imperilled.
9. The nuclear security regime should use a risk informed approach, relying on the assessment of nuclear threats and their targets and consequences.
10. The detection of nuclear security events should be ensured in order to allow appropriate response actions.
11. This requires of course also, that the corresponding authorities are prepared for the response of nuclear security events, which should be properly planned.
12. Lastly, it should be ensured that all the corresponding authorities contribute to sustaining the implemented security regime.

These twelve elements thus can only be regarded in its total in order to provide for functioning nuclear security regime of a state.

---

Nuclear security recommendations publications:

The nuclear security recommendations of the IAEA rely on the nuclear security regime set by the security fundamentals, specifying different application areas of the security regime for a more effective impact. Currently there are three recommendations:

The nuclear security recommendation on physical protection of nuclear material and nuclear facilities address nuclear threats concerning the unauthorised and unlawful removal of nuclear materials suitable for use in the construction of a nuclear explosive device. It focusses mainly on the protection of the material, but also the location and recovering of missing material. The recommendation also sets elements in order to prevent the sabotage of nuclear facilities and material, including mitigating the radioactive effects of the act of sabotage. In order to achieve this, the twelve elements of the nuclear security regime are expanded, setting specific requirements tackling the threats of unlawful removal and sabotage. Other general requirements addressing the above mentioned threats support the nuclear security regime in the physical protection of nuclear material and facilities.  

The nuclear security recommendations on radioactive material and associated facilities aim to prevent harmful acts with the intention of causing radioactive consequences, so primarily addressing the security of radioactive and nuclear material from the manufacture, storage, usage, transport (including import and export), to the recycling and disposal of the material. The recommendation also addresses the unauthorised removal of radioactive materials, but as opposed to the previous recommendation “for potential subsequent off-site exposure or dispersal.”

The nuclear security recommendations on nuclear and other radioactive material out of regulatory control is the last of the security recommendations, regulating and giving recommendations on how to handle the security of radioactive material out of regulatory control, thus “a situation where nuclear or other radioactive material is present without an appropriate authorization, either because controls have failed for some reason, or they never existed.”

This includes also stolen, or missing radioactive material that has not been reported. The recommendation sets objectives in order to provide the authorities with the effective measures in order to prevent criminal acts regarding out of regulatory control radioactive materials, but also the detection of the like and the effective response to nuclear security events involving these materials.

In order to implement an effective functioning nuclear security regime, all three recommendations go hand in hand and thus should also be considered to be implemented together.

Implementing guides:

The implementing guides for the security recommendations are more specific and apply to precise areas of the nuclear security regime and the security recommendations. There are ten implementing guides, which include for example the nuclear security culture, setting specific

---

definitions and basic concepts of the nuclear security culture in order to achieve an international consistency regarding the planning and implementation of nuclear security plans. Others address preventive and protective measures against nuclear insider threats, the security of radioactive material transportation, the security of radioactive sources, or how to detect radioactive material out of regulatory control. The two latest implementing guides address the management of radiological crime scenes and the security and confidentiality of nuclear information.

Technical guidance:

Finally the technical guidance, which also have a more additional, supportive character for the nuclear security recommendations, address specific areas of implementation or measures against nuclear and radioactive threats. These include specifications for border monitoring equipment, or for monitoring radioactive material in international mail, the identification of radioactive sources and devices, or on computer security at nuclear facilities.

All in all, the IAEA Nuclear Security Series provides a wide range of security assessment solutions tackling radioactive and nuclear threats and thus should be regarded as an important reference for all kinds of radioactive and nuclear security measures. The Nuclear Security Series are although not the only security measure recommendations by the IAEA and the department of nuclear safety and security – the IAEA also publishes for example nuclear safety standards or emergency preparedness and response series. In general, the IAEA documents provide guidance for a specific security area but they also refer to emergency preparedness and crisis management and specific CBRNE issues in these contexts. In particular this inputs, which addresses broader security areas, is regarded as a helpful asset for CRISP’s further work by the project team.

7.5. **Security of Infrastructure – Supply Chain Security**

An important part of security within the European Union is the insurance of the correct functioning of significant infrastructure – necessary for the vital social coexistence of the European citizens and also of the working of the European economy. This means that critical infrastructure facilities, as well as services ensuring the functioning of the infrastructures must be secured against internal as well as external threats. This includes supply chain security, vulnerable against all kinds of threats and for which different international security assessment solutions have been developed and implemented already. The security assessment solutions presented in this section are also related to other areas of security, mainly of border security as global cargo transportation is always closely linked with border passing and the importing and exporting of goods. Some aspects of the assessments might thus duplicate in both areas. Which is also why the presented assessment solutions is developed by the world customs organisation, who has issued an important framework of standards on global trade and supply chain security. In the following we will describe the WCO Framework of Standards to Secure and Facilitate Global Trade.

---


The WCO Framework of standards to secure and facilitate global trade (SAFE) is one of the main security assessment solutions on a global basis with the aim to harmonise customs practices by introducing a set of criteria for cargo security. SAFE was an immediate answer of the World Customs Organisation (WCO) on the events of 9/11 in the United States of America, addressing the specific needs regarding security events in customs procedures, while still maintaining, even facilitating the global trade and the flow of products across borders and continents.\(^{956}\)

The basis for the WCO framework is the WCO Kyoto Convention of 1974 (revised in 1999). Further expanding the convention with facilitated trading while strengthening the cargo security at the same time. SAFE was first adopted in 2005 by the WCO members and the framework has been improved since then. The latest version of the framework dates from 2012 – as from 2013, 168 countries have expressed their intention to implement the framework.\(^{957}\) Like other security assessment solutions, the WCO Framework can be divided into four core elements, each addressing different stages of the cargo security. First is the harmonisation of advanced electronic cargo information requirements, which inform on the incoming, outgoing as well as the transition of cargo. Risk assessment on security threats is the second element of the framework, which all signing members should implement. Thirdly, on request of a cargo-receiving country, the customs administration of the sending country should perform an inspection of the outgoing high-risk cargo through non-intrusive measures like X-ray or radiation detection. Finally the framework suggests benefits for businesses with minimal supply chain security standards which are engaging with a nation’s customs.

Furthermore, the framework draws on two important pillars of the WCO security and facilitation measures, which are Customs-to-Customs network arrangements and Customs-to-Business partnerships. Each pillar suggests a range of standards for supply chain security including technical implementation specifications, providing a good guideline for security measures.

**Customs-to-Customs network arrangements:**

Customs-to-customs network is the first pillar of the SAFE guideline for cargo security and relies to a large extend on an effective inspection and screening of cargo prior to the arrival of the transportation at the respective destination. One essential part of this inspection is the usage of the advance electronic information, identifying high-risk transportations, mainly through automated targeting tools and also require automated information exchange systems. The customs-to-customs network arrangement consists of eleven specifications: \(^{958}\)

---


958 World Customs Organisation, “SAFE Framework of Standards to secure and facilitate global trade”, June 2012, p. 9f.
### Integrated supply chain management

This specification relies already on another WCO guideline on integrated supply chain management (ISCM Guidelines). The implementation of the ISCM Guidelines allows customs administrations the request of data of the exporter for risk assessments prior importation of the goods. This includes customs control on the moment the goods enter but also leave the nation, an accompanying risk assessment (which should be shared by all the customs administrations), but also sealing by using a high-security mechanical seal.\(^{959}\)

A submission of data is necessary, which contains an advance electronic export goods declaration of the exporting country, an import declaration of the importing country and a cargo declaration of the carrier, all prior the loading of the cargo.

Time limits of the submission depends on the method of transportation and range from 24 hours prior loading for maritime containers, over 4 hours prior landing for long haul aircraft transportations, to two hours prior arrival for trains and one hour prior arrival for road transportation. When transported by maritime means, a container status message (CSM) needs also to be submitted at least 24 hours prior to the arrival at the customs administration.

Lastly an integral part of the supply chain management is an authorised supply chain which implies that all actors involved in the international trade transactions are approved by the customs administration and comply with the supply chain security specifications.

### Cargo inspection authority

The cargo administration should have the authority to inspect a cargo that originates, enters or transits the respective country.

### Modern technology in inspection equipment

The modern technology for inspection should essentially be non-intrusive inspection equipment and radiation detection equipment which are used for the inspection of the goods in accordance to the risk assessment (where available) and without the disruption of the trading and transportation process. The WCO provides guidance in form of a data base for the purchase of the equipment.

### Risk-management systems

An automated high-risk cargo identification system, including mechanisms for validating threat assessments, is an important tool for customs administrations regarding the security of supply chains. The risk-management systems should be based on best-practice examples for identification of cargo or transportation that pose a potential risk. This specification is also already included in the WCO Global Information and Intelligence Strategy.

### Selectivity, profiling and targeting

Measures and methods to identify and target high-risk cargo should be implemented, which include the advance electronic information about cargo shipments, strategic intelligence anomaly analysis, etc.

### Advance electronic information

The specification on the advance electronic information on cargo shipments include regulations on the data-exchange specifications, the usage of economic operators systems like e.g. the Cargo Community System (CCS), specifications on ICT security and digital signatures, as well as regulations on data privacy and data protection.

---

\(^{959}\) This seal has to be in compliance with the ISO 17712:2013: Freight containers -- Mechanical seals.
Targeting and communication
Administrations should initiate joint targeting which rely on standardised criteria – which will be essential for further progression of a mutual recognition of custom controls. Reference material for the targeting and communication regulations are the WCO Global Information and Intelligence Strategy, the WCO Standardised Risk Assessments document, the WCO General High-Risk Indicator document and the WCO Handbook for Customs Officers on Risk Indicators – Factors for Intellectual Property Infringement.

Performance measures
Statistical collections and evaluations of performance measures should be performed by the customs administration, including “the number of shipments reviewed, the subset of high-risk shipments, examinations of high-risk shipments conducted, examinations of high-risk shipments by Non-intrusive inspection technology, examinations of high-risk shipments by Non-intrusive inspection and physical means, examinations of high-risk shipments by physical means only, Customs clearance times and positive and negative results.”

Security assessments
Security assessments of goods involved in the supply chain, as well as transportation should be conducted together with other competent authorities in order to identify eventual missing gaps.

Employee integrity
Through specialised training, the customs authorities should ensure employee integrity on all levels and should also be able to identify eventual breaches. This includes also the installation of anti-corruption systems.

Outbound security inspections
Lastly, the customs administration should, upon reasonable request also perform inspections on outgoing custom goods, including risk assessments.

Source: Own figure
Figure 129: WCO customs-to-customs specifications

**Customs-to-Business partnership:**

Customs-to-Business partnership means essentially the engagement and partnerships of customs administrations of a nation with the private sector dealing with the security and other processes of the international trade and the supply chains. Knowing that most of the private companies dealing with supply chain security already have to comply with international security specifications, the WCO SAFE specifications on Customs-to-Business specify the requirements that are unique to cooperation with customs administrations, and are also unique to the cross-border trade of goods. The specifications of the second pillar assess the business partners of the supply chain in order to evaluate which one can obtain the authorised status of security partner – the authorised economic operator (AEO). The following six specifications should be regarded as a joint effort of the customs administration as well as of the private security company.  

---

Partnership

The AEO should engage in self-assessment processes in order to identify the best-practices and make sure to comply with international supply chain security specifications. A security plan should be established between the AEO and the customs administration.

Security

Specific security measures have to be implemented into the business model of the AEO ensuring the security of facilities through access control mechanisms and the security of trade-sensitive data through automated back-ups, information system security training and protection against unauthorised access to data. Other measures imply personnel security through regular employee screenings, but also specialised training for the employees to guarantee the security of cargo and the supply chain.

Authorisation

Through quality accreditation processes, partners will be offered incentives of being an AEO and benefit from their investments in supply chain security measures, including the contact of the customs administrations by businesses regarding concerns.

Technology

Technology specifications should entail a harmonised and facilitated trade, through the usage of advanced technology on both the customs administration as well as on the AEOs side.

Communication

The customs administration should promote the means of communication between the administration and the AEO, so that in case of a security breach or necessary emergency measures, the suitable customs administration unit can be contacted efficiently. But also the regular consultation on all matters of security issues should be initiated with all partners involved. This means also that the AEO partner should be open to the coordination of those matters through the customs administration.

Facilitation

In order to facilitate cross-border trade, the partnership between the customs organisation and the AEO should also be facilitated by means of cooperation on both sides, including mechanisms that allow AEOs to comment on proposed regulations and amendments of supply chain security measures by the customs administration.

Source: Own figure

Figure 130: AEO specifications

The WCO SAFE framework is a very good example on the wide variety of measures that need to be implemented at the area of customs organisation in order to provide an effective supply chain security. Furthermore it shows clearly the large amount of different steps involved in the transportation process and thus also the different stages where security threats can be induced and security measures need to be implemented. Since the amended Kyoto Convention is the basis of the WCO SAFE, a lot of references are made to the Kyoto Convention, within which some of the aspects are further specified and implementation models are provided.962

The WCO SAFE framework was in the last years further developed in order to be part of the WCO SAFE package, including a number of guidelines, support material and instruments for the implementation of the framework. All in all, the work of the WCO regarding the supply chain security can be a good basis for other standardisations and implementations of security measures within this area.

7.6. SECURITY AND CRISIS MANAGEMENT

Standardisation and certification processes in the area of crisis management are not always easy to implement. While technical requirements, which apply to the range of security products and systems often are easily identified, this is not always the case for crisis management. Here the importance of the requirements lies on the ways, security professionals have to react in case of emergency, as well as on strategic and day-to-day handling of (possible) security threats. There is a link between security assessment solutions of crisis management services and private security services, as it requires recommendations of how people involved should be able to conduct in certain situations. In the following we will provide information on the American Society for Industrial Security (ASIS).

ASIS offers certification of Physical Security Professionals. A general description of the outcomes of the certification process and the desired capabilities is available online as well as in this report’s country study ‘United States’. Security assessment in this framework primarily takes the form of vulnerability analysis: the certification should demonstrate detailed competencies in risk analysis and threat assessment. Also, it aims at a better understanding of integrated physical security systems. This assessment scheme also builds on a holistic management approach to security measures, involving their identification, implementation and continuous evaluation. On the website, ASIS also provide a definition of physical security. It centres on the sum of existing measures which have been put in place to safeguard people, assets and information. Thus, this approach to (physical) security entails a strategic component (scanning for and analysing risks and threats) and a day-to-day, managerial component, which is concerned with the implementation of measures (according to the definition, predominantly systems and systems of systems) and the evaluation of effectiveness.

ASIS also developed a “General Security Risk Assessment Guideline”. The scope of this guideline is “any environment where people and/or assets are at risk for a security-related incident or event that may result in human death, injury, or loss of an asset”. The Guideline is also geared at security professionals. It is meant to empower them to not only identify security risks at a specific site, but also to communicate them. It also details the seven steps for a thorough security risk assessment:

1. Understand the organisation and identify the people and assets at risk;

---

965 ASIS International, op. cit., 16.03.2015.
2. Specify loss risk events and vulnerabilities;
3. Establish the probability of loss risk and frequency of events;
4. Determine the impact of events;
5. Develop options to mitigate risks;
6. Study the feasibility of implementation of options;
7. Perform a cost/benefit analysis.

The document also provides a helpful list of sources, which should be drawn upon for the determination of loss risk events.

ASIS nicely shows how certification for a specific purpose – here physical security professionals can also be used for other, related situations like in crisis management. This also shows that there is a kind of similarity regarding security related services in general, where it obviously very difficult to implement specific standardisation guidelines, but therefore holistic approaches are easier to implement. The opposing aspect of the holistic approach for security related services – including crisis management – consists of the low specificity of the recommendations.

7.7. **Border Security in General**

Lastly the area of border security is a sector in which a large amount of international security assessment solutions were established in the last 15 years. As a reaction of the 9/11 events, a lot of policies aiming at securing the flow goods and persons across borders have emerged. Many of the security solutions originate from the U.S. and were adopted subsequently by other countries and partners. Since most of the policies target cargo security, and here also specifically maritime cargo transportation security, chapter 7.8 specifically addresses maritime boarder security, while in this chapter we focus on cargo and person security at land and air borders.

It is important to note that the term border security used here relates more to border control or border monitoring of the flow of goods and people across borders as to border security in terms of state legitimacy and sovereignty against other states in moments of conflict. Precise definitions of the term border security are often missing, which is also criticised by Kathleen Walsh as a missing common definition “remains an obstacle to increased implementation of border-focused international initiatives.”

---

7.7.1. **Passenger Name Record Data**

International security solutions on land and air border aiming at the monitoring of the flow of people are for example the passenger name record (PNR) data, which consists of personal information provided by a passenger when booking a flight and checking-in to that flight. This data can be used by law enforcement authorities for the fighting of crime and terrorism by detecting, investigating and prosecuting perpetrators.\(^{968}\) The systematic EU-wide collection, usage and retention of PNR data is currently discussed on the level of the council of the EU and the European parliament. While proponents highlight the possibilities and advantages in fighting terrorism and (organised) crime, the opponents fear violations of privacy rights.\(^{969}\) An agreement between the U.S. and the EU on the use and transfer of PNR data to the U.S. home department exists already since 2011.\(^{970}\)

The efficiency of the passenger data collection and usage for the fighting of crime and terrorism although needs to be discussed. The international organisation for migration highlights the importance of cross-agency and international collaboration for maximising the efforts in border security and mentions the National Border Targeting Centre (NBTC) of the UK as a good example: “The Centre brings together analysts from the UK Border Agency, the police and security services to monitor travel into and out of the UK, including to and from EU Member States, to identify people of immigration or criminal/terrorist interest who threaten the UK. It also helps build intelligence for those agencies involved.”\(^{971}\) Nevertheless, reports from the Home Affairs Committee in the UK on the work of the UK Border Agency note some serious failures concerning the NBTCs usage of the passenger data. In the sixth report of session 2012–13, the committee notes that while a large number of security alerts by the NBTC are being issued, the passengers identified as a potential threat are not being intercepted.\(^{972}\) In the eight report of session 2013–14, the committee reports that during a ten month period around “650,000 alerts about smugglers of drugs and other contraband, as well as tax avoiders, were deleted without being read by staff at the National Border Targeting Centre.”\(^{973}\)

Although this is only one example of many it is obvious that data collections – in this case passenger data – are not a recipe for the successful fight against cross-border crime and terrorism or illegal migration. International cooperation which does not only rely on data collections might be more useful in this area.

---


7.7.2. CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM (C-TPAT)

One of the international cooperation mentioned in the previous sub-chapter is the Customs-Trade Partnership Against Terrorism (C-TPAT). C-TPAT was launched by the U.S. Customs and Border Protection (CBP) shortly after 9/11 as a reaction to the terrorist attacks: “One of the best means to prevent further terrorist attacks is to use border authorities to make it more difficult for terrorists or terrorist weapons to enter the United States to carry out attacks.” The partnership initially aims at securing the U.S. border and the trade to and from the USA, but the involved partners are meanwhile internationally widespread. The strategy of C-TPAT is to voluntarily involve all partners of the supply chain in the assessment and enhancement of security – “extending the United States’ zone of security to the point of origin.”

The C-TPAT offers a wide set of minimum security requirements which partners in the programme must meet in order to be eligible for participation. The minimum security criteria and guidelines cover requirements, which apply to general security procedures of the partner, especially regarding the proceeding with business partners (for example for screening of cargo and cargo/container security). But the security criteria also set minimum requirements for access control security, personnel security, physical and IT security, as well as security training and threat awareness.

These minimum security criteria and guidelines are available for all the different actors in the supply chain, covering foreign manufacturers, highway, rail, air and sea carriers, third party logistics providers, long haul carriers in Mexico, importers, exporters, customs brokers, marine port authority and terminal operators, as well as consolidators (air freight consolidators, ocean transport intermediaries, and non-vessel operating common carriers (NVOCC)). All these actors must meet the specific security requirements, if they want to be part of the C-TPAT and become a certified partner.

The strategy of C-TPAT consists of a five goal programme, each with different approaches and objectives to the partners in order to achieve a rise in cross-border security:

- **Goal 1:** Ensure that C-TPAT partners improve the security of their supply chains pursuant to C-TPAT security criteria.

The first goal, as well as the second goal of the C-TPAT programme especially address the outside partners involved in the supply chain to the U.S. This implies, that the partners contribute to the supply chain security and fulfil the minimum security criteria. By signing the agreement, the partners commit themselves to collaborate with the CBP and implement best practice security measures, which address topics like personnel security, access controls, special training, threat awareness, etc. C-TPAT partners can undergo a review process in order to become certified partners by the U.S. CBP – the certification is required for partners in order to profit from programme benefits presented in Goal 2.

---

In a second step after certification, the partner will be validated by the CBP, in which it is made sure that the participant security plans and enhancements are effective. A joint-review by the CBP and the C-TPAT partner allows to evaluate implemented security measures and to promote information exchanges between both the CBP and the partner company on best-practice examples and security issues. The advantage of the C-TPAT is its flexibility in adapting the scope of the certification and validation processes, from certain parts of the supply chain, to manufacturer sites and external logistic suppliers, depending on security threats and necessities. Further compliance with the C-TPAT procedures are achieved through systematic reviews by the partners, which are mainly carried-out through regular self-assessments.

**Goal 2: Provide incentives and benefits to include expedited processing of C-TPAT shipments to C-TPAT partners.**

Incentives and benefits for the C-TPAT partners are manifold. The CBP provides all certified partners with a secure communication platform, on which security and threat assessments, intelligence reports, partnership and member statutes are shared and can be accessed. Best practice examples, reported by certified members are made available to the other members. Communication is an essential part of the partnership and thus promoted on several ways. Regular conferences, with the members or the trade community in general are for example also important channels of communication by the CBP. Security training specifically for supply chains is also provided by the CBP, in which security experts organise training initiatives for the partners which include methods for the better inclusion of the C-TPAT programme goals.

Beside communicational and training benefits, the partners also profit from processing benefits in the supply chain. The required minimum security standards, to which all the C-TPAT members must comply, address all the steps in the supply chain – from the point of origin, through the cargo process, to the arrival. The benefit of sticking to this process result in accelerated processes by reduced inspections and the “FAST lane clearance.” The Free and Secure Trade (FAST) lanes are special lanes at multiple points at the land borders between the USA and Canada, as well as the USA and Mexico, specially established for C-TPAT members, who are considered as low risk and thus can pass with lower examination rates.

**Goal 3: Internationalise the core principles of C-TPAT through cooperation and coordination with the international community.**

As already note in the introduction, C-TPAT is mainly an U.S. initiative, which also reflects in most of the members being companies located in the United States of America. Goal 3 aims (or aimed) at the internationalisation of the partnership through the cooperation with international partners. The international trade made it necessary to include certain steps also into the C-TPAT programme, which mainly focuses on the implementation of the supply chain security standards to other – foreign and overseas – companies, who have a cooperation with C-TPAT members.

Also cooperation by the CBP with other customs administrations are part of the internationalisation of the C-TPAT requirements, which have resulted in different other programmes, like

---

the container security initiative (CSI), which will be presented in Chapter 7.8.3. The implementation of similar C-TPAT programmes at foreign customs administrations is also part of the internationalisation, as it simplifies the collaboration between the administrations if common security requirements are implemented. Another international cooperation through the C-TPAT programme is between the CBP and the world customs organisation (WCO), where the C-TPAT office participated for example in the development of the SAFE Framework (see chapter 7.5).

One of the results of Goal 3 are the mutual recognition arrangements between the CBP and other customs administrations on supply chain security requirements. These agreements are mainly initiated with the U.S. top trading partners, like Canada, Mexico, the EU, or Japan. So far ten mutual recognition arrangements have been signed by the CBP – with similar benefits as the general C-TPAT benefits: a lower risk score on cargo, common security and trade standards and an increase in transparency.  

Goal 4: Support other CBP security and facilitation initiatives.

The support of other CBP security and facilitation initiatives include programmes like the FAST programme, which accelerates the land transportation between the USA and Mexico and the USA and Canada, from which C-TPAT partners can benefit. Also the support of the CSI programme is seen as essential by the CBP for the C-TPAT partnership. Other initiatives are the development and implementation of secure and smart containers. Containers are the centre of the supply chain, as they allow to protect the merchandise but are often also misused by smugglers. Minimum security requirements for containers thus need to be implemented in order to prevent the misuse of containers for smuggling activities, as well as the improvement of the security of the merchandises. The CBP can build here on the security criteria established for the C-TPAT programme. Further initiatives are antiterrorism initiatives between the CBP and the DHS as for example the Carrier Initiative programme (CIP), Business Anti-Smuggling Coalition (BASC) and Americas Counter Smuggling Initiative (ACSI).  

Goal 5: Improve administration of the C-TPAT programme.

Lastly the fifth goal of the C-TPAT programme is the improvement of the administration. On the one hand, an implementation of a human capital plan should assess the annual workload, as well as the average validation time supply chain security specialists require for validations. This will allow to evaluate the necessity of specialists for a certain time period. On the other hand, (update) training programmes for the specialists ensure the preparedness for new challenges in the supply chain security. Administration can also further be improved through enhanced data collection and information management capabilities.

Overall, the C-TPAT programme can be seen as a good practice example, of how customs administrations can improve their supply chain security, by not only investing themselves in security improvement measures, but by including a wide range of members and participants in the process – and providing initiatives for the cooperation with the programme. C-TPAT also nicely shows the internationalisation of the supply chain, which also affects its security and

---

which thus needs to be addressed by a wider collaboration between customs administrations, import/export providers and manufacturers.

7.8. **BORDER SECURITY – MARITIME SECURITY**

In 2013 9.580 million tons of cargo were transported by sea,\(^{981}\) which represent for decades the largest part of the global cargo transportation. While a lot of this trade happens hidden from the public image, the importance of the security of this area is evident. This relates of course to the security of infrastructure: port facilities and supply chains are the main part of the maritime cargo transportation. But with the huge internationalisation of cargo transportation, the maritime trade is also highly relevant to the aspects of border security. This was already shown by the C-TPAT initiative and will also be highlighted by the Container Security Initiative (CSI). Both are security assessment solutions of the U.S. Customs and Border Protection, which strongly focus on protecting the national maritime borders by increasing the security measures of the international maritime trade.

This is also the reason to include both initiatives here – although being originally U.S. measures, the requirements have a global wide impact. But also the work of the International Maritime Organisation (IMO) should be highlighted here, which is one of the most important promoters of security requirements in the maritime area. With the International Ship and Port Facility Security Code, we present security requirements which have subsequently been implemented on a European scope in the Regulation 725/2004 enhancing ship and port facility security.

7.8.1. **INTERNATIONAL SHIP AND PORT FACILITY SECURITY CODE**

The International Ship and Port Facility Security (ISPS) Code was established by the international maritime organisation (IMO). It is a part of the Safety of Life at Sea (SOLAS) and thus compliance with the ISPS is required for all parties of the SOLAS. The ISPS code sets mandatory maritime security measures, setting minimum and harmonised requirements for securing the international maritime transportation and thus needs to be implemented in national legislations of the countries participating in the SOLAS.

The basic understanding of the ISPS is that an increase in ship and port facility security can be achieved through risk management, investigating each potential security threats and risks in order to evaluate the adequate security measure. Thus the ISPS code provides “a standardized, consistent framework for evaluating risk, enabling governments to offset changes in threat levels with changes in vulnerability for ships and port facilities.”\(^{982}\) Functional security requirements, like security plans and access control systems are examples of security measures which are addressed by the ISPS code.

One other important aspect of the ISPS is maintaining security awareness. As a lot of security measures have been implemented, the general feeling of security amongst port facilities has risen subsequently. Without neglecting the positive aspect of this, it is necessary that a general

---


awareness of the risks ports and especially maritime cargo transportation might be confronted with. This is also why the ISPS code promotes security awareness as part of training programmes for port facility security personnel and ship security officers.983

As noted, the ISPS code requires implementation in national legislations, which has been accomplished on a European basis by the Regulation 725/2004 addressed in the next chapter (see Chapter 7.8.2). The ISPS does not only set security recommendations for national governments and national authorities, but also to port as well as ship operators, covering all the aspects of the maritime transportation, from the governmental and authoritative part of port facilities, to the private organisations and companies operating port facilities and ship transportation.

Most of the requirements of the ISPS deal with the security assessments which apply to the port facilities and the maritime transportation. For that reason the IMO provides a security assessment framework, in order to give guidance on the security assessment to the involved parties.984 The security assessment framework of the IMO covers the commonly used phases of the assessment (mainly pre-assessment, threat assessment, impact assessment, vulnerability assessment, risk scoring, and risk management) and gives adequate guidance, including specifically designed templates with threat scenarios corresponding to the maritime environment.

Overall the ISPS code presents a wide range of security requirements, of which especially the approach of the security assessment in order to address the possible threads stands out and can be regarded as a best practice example, not only for maritime border settings but also other areas of security.


As already mentioned in the previous chapter, the Regulation 725/2004 implements the requirements of the International Ship and Port Facility Security Code on the European level. By the implementation of the ISPS through a regulation, the European Union applies the ISPS code and the security requirements not only on the international maritime transportation but also on the inner-European maritime transportation.

The Regulation starts by quoting terrorism and, more generally, intentional unlawful acts as the main threats to the EU’s security and its values. The Regulation is to be implemented against such threats. It provides for the description of the main contents as well as a generic methodology of security assessments for port facilities and ships. In principal, such assessments should lead to the development of security plans intended to empower operators to flexibly react to fluctuating levels of security.

What does the Regulation mean by “plan”? With regard to a ship, a security plan denotes “a plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship’s stores or the ship from the risks of a security incident”.985 In a nutshell, therefore, the security plan, as it results from a security

assessment, is about measures, preventive protection, implementation, risks and security-critical “incidents”. The latter, read in light of the introductory remarks, probably to denote the threat by the intentional actor (which is, however, not specified for the development of the plan. However, §2 of the preamble mentions piracy as one of the conceivable threats.\footnote{European Parliament and the Council, op. cit., 21.03.2004, p. 6.}

There are several key functions in this process:

- gathering and assessing information with respect to security threats and exchanging such information with appropriate Contracting Governments;
- requiring the maintenance of communication protocols for ships and port facilities;
- preventing unauthorised access to ships, port facilities and their restricted areas;
- preventing the introduction of unauthorised weapons, incendiary devices or explosives to ships or port facilities;
- providing means for raising the alarm in reaction to security threats or security incidents;
- requiring ship and port facility security plans based upon security assessments; and
- requiring training, drills and exercises to ensure familiarity with security plans and procedures.

In the case of a ship security assessment, the Regulation provides the following elements:

- identification of existing security measures, procedures and operations;
- identification and evaluation of key shipboard operations that it is important to protect;
- identification of possible threats to the key shipboard operations and the likelihood of their occurrence, in order to establish and prioritise security measures; and
- identification of weaknesses, including human factors, in the infrastructure, policies and procedures;

The overall ship security assessment process is to lead to a ship security plan. The regulation outlines the minimum requirements such a plan has to comply with. They are:

- measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorised from being taken on board the ship;
- identification of the restricted areas and measures for the prevention of unauthorised access to them;
- measures for the prevention of unauthorised access to the ship;
- procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;
- procedures for responding to any security instructions Contracting Governments may give at security level 3;
- procedures for evacuation in case of security threats or breaches of security;
- duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;
- procedures for auditing the security activities;
• procedures for training, drills and exercises associated with the plan;
• procedures for interfacing with port facility security activities;
• procedures for the periodic review of the plan and for updating;
• procedures for reporting security incidents;
• identification of the ship security officer;
• identification of the company security officer, including 24-hour contact details;
• procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board;
• frequency for testing or calibration of any security equipment provided on board;
• identification of the locations where the ship security alert system activation points are provided; and
• procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts.

The methodology for port facility assessments parallels the actions described above.

7.8.3. **Container Security Initiative (CSI)**

The Container Security Initiatives (CSI) is, similar to the C-TPAT programme, initially an USA based security assessment solution, which was introduced in 2002 as a reaction to the 9/11 terror attacks by the U.S. Customs and Borders protection. With the aim of the protection of the most important part of the global trade – the shipping of containers – CSI addresses the threats to which maritime containers are exposed, mainly in the area of illegal trafficking of people, drugs, and weaponry. While the identification of high-risk containers is one of the core elements of the CSI, the modus operandi of pre-screening and evaluation of the containers prior shipping needs to ensure not to slow down the trade throughout the process. This is one of the main challenges the security of containers has to challenge.

Since about 95% of the imports to the U.S. (in 2005 this corresponded to 11 million containers being offloaded at ports in the USA), the protection of the containers and subsequently of their port facilities is highly important – and cooperation with other customs administrations and port facilities in order to effectively fulfil this task is crucial. So far, the CBP cooperates with 58 ports which also have implemented the CSI and corresponds thus to 80% of the maritime cargo containers which are pre-screened prior importation to the USA.

An interesting insight in the functioning of the CSI gives the strategic plan 2006-2011, which was designed at addressing the essential elements of terrorist threats to the maritime trade – categorised in three strategic goals:

**Goal 1: Secure U.S. Borders:**

The first goal of the strategic plan is the security of the U.S. Borders – since the CSI was mainly introduced in order to protect the maritime trade into the USA. Especially important for the CSI here is the identification of high-risk cargo, which is one of the main tools of the
cargo security. In order to successfully identify high-risk cargo, the receiving port requires the receiving of cargo information prior arrival, which is regulated by the 24-hours rule. This requires lading information 24 hours prior the loading of the cargo on the ship at the foreign port. This is supported by the automated targeting system (ATS) of the CBP which applies targeting rules to the incoming freight and assigns a risk level to the cargo prior leaving the foreign port. Further information, obtained in collaboration with other ports and customs administrations are also included into the ATS, with the result of a better targeting of high-risk cargo and a reduction of false-negatives.

Other tools for identifying high-risk cargo involve the process of screening and examining of the containers. The usage of state-of-the-art methods and technologies, combined with close collaborations with interagency programmes (e.g. U.S. Coast Guard International Ship and Port Facility Security (ISPS) Code) and foreign customs administrations and ports are the main assets here. Technology-wise it is important that non-intrusive inspections are efficient in detecting threats upon screening. Also methods of physical inspection, as a result of detecting a threat are important to efficiently improve. A flow-chart of how the screening process is done and what steps are taken upon high-risk identification and anomaly detection can be seen in Figure 131130.

![Diagram of CSI screening process of containers](image)

In order to achieve that this screening process is conducted efficiently and equally at all the CSI ports, a coordinated collaboration between the CBP and the ports is important. Personnel

---

and technological presence of the CBP at CSI ports around the world, as well as information and trade data sharing contribute to achieve parity between all the ports.

**Goal 2: Build a Robust CSI Cargo Security System:**

The second goal connects to the first on, since with the container security initiative, the CBP aims at promoting a global cargo security system, in which the detection of threats through state-of-the-art technologies are carried out by the host/cargo sending country – all based on harmonised standards through a common international framework. Also a common examination and security process should be promoted globally, for example through “a common risk-management approach regarding the way high-risk containers are identified.”

Also global technology standards can contribute to a harmonised cargo security system. Especially the World Customs Organisation (WCO) with its 169 members is an important asset here.

Also the selection of the ports, to which the CSI should apply can help for the security of the maritime cargo trade. The important factors here are essentially the volume of trade of the port with the importing country, the possible connections of terrorist groups with the location, and geographical significance of the port.

As important as the identification and detection of high-risk cargo is, as important is also the effective and quick movement of low-risk cargo. The CSI can contribute greatly to this, but therefore it is important that all partners effectively contribute to this in order to guarantee the flawless transportation of the low-risk cargo. Important is here also the close cooperation with other agencies on maritime security, be it with home security agencies, LEAs, public and private agencies, in order to promote methods and initiatives for securing the global maritime containerised trade.

**Goal 3: Protect and Facilitate Trade:**

The third goal recapitulates some of the aspects already addressed in the first two goals. The facilitation of trade can only be effectual if the cooperation between the ports is guaranteed, information sharing is equally established and the process as described in Figure 131130 is carried out. For this it is of course important that periodic risk assessments of the CSI ports are conducted, the required staff is well trained and the equipment is available and also regularly revised. Also new ports which are included in the CSI need to be modified accordingly, in order to meet the security requirements.

Trade data sharing as well as other information sharing, as for example watch-lists, should not only be limited to the exporting and importing CSI port, but should also be shared with the other CSI ports. Information gathering can furthermore be done collectively with other organisation, like for example nuclear safety agencies. This will contribute to an effective functioning of the automated targeting system for the identification of high-risk cargo.

The promotion of the available CSI standards to other international organisations and governments, involved in maritime (trade) security, as well as the participation in the development of further standards also contributes to the effectiveness of the container security initia-

---

tive and the facilitating of secure maritime trade. Here it would be important to give initiatives for participation and increase the awareness for the need of a secure global trade.

As is shown, the CSI provides an effective example in improving the security of maritime containerised trade, which is represents the largest amount of trade world-wide. While the most important part of the CSI is the container screening prior shipment to the importing country, possibilities for standards are especially in the process of examination – which could be included in port security standards in general. Although the CSI was initially targeted at improving the U.S. maritime border security and maritime cargo transportation, it contributes globally to the reducing security threats on the maritime supply chain – and can also serve as an example for the implementation of similar initiatives in a European context.
7.8.4. INFORMATION SECURITY - COMMON CRITERIA

7.8.4.1. INTRODUCTION

In this section we look at the Common Criteria framework for Information Security products. We examine briefly the ISO/IEC 15408 on which the Common Criteria framework is based and then we discuss the key concepts of the Common Criteria. Finally, we look at three selected Common Criteria Certification Schemes, the Dutch, Canadian and Indian schemes and we conclude with the success factors and the limitations of the framework.

The ISO/IEC 15408 is the base of the Common Criteria version 2. The first version was published in 1996, as a result of the integration of information technology and computer security criteria.991

The ISO/IEC 15408 “Information technology -- Security techniques -- Evaluation criteria for IT security” contains a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation.992 It consists of three standards; part one, revised in 2009, establishes the general concepts and principles of IT security. It also specifies a model of evaluation for security properties and IT products.

The second part of the ISO/IEC 15408:2008, reviewed in 2014, defines the content and presentation of the security functional components to be assessed in the security evaluation based on the ISO/IEC 15408. This part of the standard, also provides guidance on customised requirements. The third part, the ISO/IEC 15408:2008, also reviewed in 2014, defines the assurance requirements of the evaluation criteria.993

7.8.4.2. THE COMMON CRITERIA FRAMEWORK

Background

As discussed in the CRISP report on security standards and certification in Europe, Common Criteria is the result of the combined efforts of a number of governments to develop harmonised security criteria for Information Technology products.994,995 The criteria provide the technical basis for an international agreement that provides for mutual recognition of certification of secure Information Technology products.996

References:

The Common Criteria scheme is government-driven. Private actors such as CBs and Testing Laboratories might also participate in the schemes. In this way, public and private actors, ministries, the industry and other bodies cooperate under the Common Criteria scheme in order to achieve its goals.

According to the National Information Assurance Partnership, Common Criteria is a framework in which:

- Government, military and other users can specify their security functional and assurance requirements through the use of protection profiles,
- Vendors can then implement and/or make claims about the security attributes of their products, and
- Testing laboratories can evaluate the products to determine if they actually meet the claims.

The scheme is subject to revisions, since it needs to respond to new risks posed by the misuse of technological evolution. The participant countries are divided in Certificate Authorising Participants and Certificate Consuming Participants. The former recognise mutually the certificates issued by the other Certificate Authorising Participants. Certificate Consuming Participants, although they may not maintain an IT security Evaluation capability, nevertheless have an expressed interest in the use of certified/validated IT Products and Protection Profiles.

The CCRA provides the conditions for mutual recognition by the participant countries of the Common Criteria certificates issued in any of the authorizing countries of the Common Criteria framework. Recently, the signified members agreed to a revision of the Common Criteria Recognition Arrangement. The purpose of the revision was “to raise the general security of certified information and communications technology products without increasing costs or preventing timely availability of such products from commercial companies.”

The revised CCRA foresees mutual recognition of the certificates of Evaluation Assurance Levels from EAL1 to EAL2 and Collaborative Protection Profiles. With assurance activities from Evaluation Levels from EAL1 to EAL4. Article 5 sets the conditions for the recognition, which include that the certification process has been carried out on the basis of accepted IT Security Evaluation Criteria; using accepted IT Security Evaluation Methods and Supporting Documents; the scheme is managed by a compliant Certification Body in the Certificate Authorising Participant’s Country and that the certificates issues satisfy the objectives of the Arrangement.

---

1000 new CCRA signed in July 2014, see further below
Common Criteria Overview

The Common Criteria consists of the Introduction and description of the general model (Part 1), the Security Functional Components part (Part 2) and the Security Assurance Components Part (Part 3).\textsuperscript{1003}

As general purposes of the Common Criteria are set the following:

1. To ensure that evaluations of Information Technology (IT) products and protection profiles are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and profiles;
2. To improve the availability of evaluated, security-enhanced IT products and protection profiles;
3. To eliminate the burden of duplicating evaluations of IT products and protection profiles;

\textsuperscript{1002} Common Criteria, Members of the CCRA, no date. https://www.commoncriteriaportal.org/ccra/members/
4. To continuously improve the efficiency and cost-effectiveness of the evaluation and certification/validation process for IT products and protection profiles.

The Common Criteria addresses mainly three aspects of IT security: confidentiality, integrity, and availability. It addresses the protection of assets from unauthorized disclosure, modification, or loss of use. Additionally, it is applicable to risks arising from human activities (malicious or otherwise).

Figure 133: Common Criteria logo

Interested parties

The Common Criteria targets several categories of audience. First, the consumers are in the core of the framework. The first part of the CC framework states that the CC is written to ensure that the evaluation fulfils the needs of the consumers. Users and consumers can benefit from the common criteria in the sense that they can rely on an independent third party evaluation results based on internationally accepted criteria and not depend solely on the information provided by the vendor. Also, procurers use the common criteria to structure the security requirements of the procurement calls for information systems. Another target group of the CC is the developers, i.e. the organisation responsible for the development of the Targets of Evaluation (TOE) and the manufacturers.

Key Concepts

Protection Profiles (PP)

A Protection Profile defines a set of security requirements and objectives for a type of products or systems which meet similar consumer needs for IT security, e.g. firewall. The set of security requirements is independent from the actual implementation. The PP is intended to be reusable and to define requirements which are known to be useful and effective in meeting the identified objectives. The PP concept has been developed to support the definition of functional standards, and as an aid to formulating procurement specifications.

---

1006 A TOE is defined as a set of software, firmware and/or hardware possibly accompanied by guidance: Part 1 of CC, p. 32
Security Target (ST)

A security target contains the IT security objectives and requirements of a specific Target of Evaluation and defines the functional and assurance measures offered by that TOE to meet stated requirements. The ST may claim conformance to one or more PPs, and forms the basis for an evaluation.\textsuperscript{1007} The ST is the basis for the agreement between the TOE developers, consumers, evaluators and evaluation authorities as to what security the TOE offers, and on the scope of the evaluation.\textsuperscript{1008}

Evaluation Assurance Level (EAL)

The Evaluation Assurance Level defines how thoroughly the product is tested. Each EAL has a unique name, which provides information on the intent of the EAL. "The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance."\textsuperscript{1009} The following figure shows the seven hierarchical EALs which are defined in order to rate the assurance of the TOE.

<table>
<thead>
<tr>
<th>Type of EAL</th>
<th>Type of Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAL1</td>
<td>Functionally tested</td>
</tr>
<tr>
<td>EAL2</td>
<td>Structurally tested</td>
</tr>
<tr>
<td>EAL3</td>
<td>Methodically tested and checked</td>
</tr>
<tr>
<td>EAL4</td>
<td>Methodically designed, tested, and reviewed</td>
</tr>
<tr>
<td>EAL5</td>
<td>Semiformally designed and tested</td>
</tr>
<tr>
<td>EAL6</td>
<td>Semiformally verified design and tested</td>
</tr>
<tr>
<td>EAL7</td>
<td>Formally verified design and tested</td>
</tr>
</tbody>
</table>

Source: Own figure, Common Criteria, part 3
Figure 134: Common Criteria evaluation assurance levels and content

EAL1 is the lowest Evaluation Assurance level of the Common Criteria. It represents that functionality is tested and that due care has been exercised with regard to the protection of personal or confidential information. The security target needs to be limited, as the level of assurance is basic. EAL2 provides assurance by a full security target; it requires developer testing, vulnerability analysis and independent testing. Building up to EAL7, every level requires additional assurances. EAL7 is applicable to extremely high risk situations. The value of the assets justifies the selection of this evaluation level.

\textsuperscript{1008} Common Criteria, op. cit., p. 15
\textsuperscript{1009} Common Criteria, Part 3, op. cit., p. 30
In 2012, the Common Criteria Recognition Arrangement (CCRA) Management Committee issued a vision statement for the future direction of the Common Criteria and the CCRA. This vision statement highlights a shift from Evaluation Assurance Levels to Protection Profiles, which means that all products of a type will be evaluated against the same claim and moves away from the notion that one product is evaluated against rigorous set of requirements. This is due to the fact that Protection Profiles do not identify a prescribed assurance level; instead they include prescribed assurance measures and test requirements. As a result, the Common Criteria are moving towards a technology specific, tailored assurance requirements.

7.8.4.3. COMMON CRITERIA CERTIFICATION SCHEMES

As shown in Figure 132131, Common Criteria certification is conducted in 17 countries. This sub-chapter illustrates national examples of Common Criteria Schemes in three continents (Europe: the Netherlands, North America: Canada and Asia: India).

Netherlands

The Dutch common criteria certification scheme, Netherlands Scheme for Certification in the Area of IT Security (NSCIB), is operated by TUV Rheinland Nederland B.V I in cooperation with the Ministry of Interior and Kingdom Relations. In 2000, the Dutch government provided permission to the Netherlands National Communication Security Agency for the development of the scheme for the Netherlands on behalf of the Dutch government. TUV is the Certification Body of the scheme. The scheme is compliant with both the Common Criteria Recognition Agreement and the European SOG-IS Mutual Recognition Agreement.

The Dutch government signed two agreements under the Common Criteria Scheme:

a) The common criteria recognition arrangement (CCRA) signed in 2000 by the Netherlands, which provides recognition up to EAL4.

b) The European SOGIS-Mutual Recognition Agreement, which provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products.

Agreement b) is in particular signed by Finland, France, Germany, Norway, Spain, Sweden, the United Kingdom, Italy and the Netherlands. What is different with regard to the schemes of the other two countries examined under this section, is that for the products in the

---


1012 Website of the scheme: http://www.tuv-nederland.nl/nl/36/certification.html

1013 Common Criteria Management Committee, Mutual Recognition Agreement of Security Evaluation Certificates, v.3.0, January 2010

1014 The SOGIS-IT-Technical Domains-v.0.93 lists the technical domains concerned by the agreement for the high level of recognition; these domains are “smart cards and similar devices” and “hardware devices with security boxes”: http://www.sogisportal.eu/documents/mra/SOGIS-IT-Technical-Domains-v0.93.pdf
technical domain of smart cards and similar devices, the Dutch scheme provides a higher recognition level for evaluation beyond EAL4. The NSCIB consists of five parts:

a) The introductory part, providing an overview of the objectives, the organisation and the procedures of the NSCIB.

b) The second part regulates the certification itself, the processes the roles and responsibilities of the actors.

c) The third part describes the process according to which an Information Technology Security Evaluation Facility (ITSEF) is licensed.

d) The following part concerns the roles in the Certification Body.

e) The last part provides templates for reports e.g. Evaluation Technical Report template, documents e.g. a certificate template, the application form etc.

The documentation of the certification scheme includes the Common Criteria sections and additionally the General Regulations of TUV Rheinland Nederland. The latter are indicated with different font in the text. For example, the clause 3.1. regarding premature termination of the certification process is part of the TUV Rheinland Nederland General Regulations.1015 The same is partly for the security (confidentiality and integrity), the cost of certification, and use of the international certification marks sections of the Dutch scheme.1016 With regard to the interpretation of specific parts of the NSCIB, apart from the application guides of the common criteria, the Common Criteria supporting documents and the Guides issued by the JIL Working Group, the Certification Body provides with additional “national interpretations”. The national interpretations documents relate mainly to technical issues, such as the site audits, the testing, the composite evaluations, but also other topics such as the consultancy services of the Certification Body.1017,1018

Canada

The Canadian Common Criteria Certification Scheme (CCS), is a partnership between government and industry. The technical oversight of the evaluation and the certification of the results is performed by the Certification Body within the government of Canada and is operated by the Communications Security Establishment Canada. The evaluations are conducted by approved private-sector evaluation laboratories. The CC evaluations in Canada reach up to level EAL4. Among the objectives of the scheme is the effective IT security evaluation capability in Canada and the maximum possible IT security to the departments and agencies of the Government of Canada. The Canadian scheme therefore highlights the territorial focus of the CCS and its value for the IT security of the Canadian government itself.

---

1015 Section 3.1. of the NSCIB Scheme Documentation, version 2.1, 01-08-2011 p. 29/73
1016 NSCIB, op. cit., Sections 3.4., 3.5., 4.3.
1017 TUV Rheinland Nederland and Ministerie van Buitenlandse Zaken en Koninkrijksrelaties “Netherlands Scheme for Certification in the Area of IT Security (NSCIB), NSCIB Scheme Interpretation #1, Performing Site Audits”, http://www.tuv-nederland.nl/upload/pages/33/NSI%201%20Performing%20Site%20Audits%20v2.1.pdf
The CCS consists of five guides on the Scheme Description, Quality Manual, Evaluation Facility Approval, Technical Oversight for TOE (Target of Evaluation) Evaluation and Technical Oversight for Assurance Continuity of a Certified TOE.

Canada has four evaluation facilities, which are accredited by the Standards Council of Canada under the Information Technology Security Evaluation and Testing programme, and are licensed by the Canadian Certification Body to carry out Common Criteria evaluation activities.

India

The Indian Common Criteria Certification Scheme, IC3S, which was presented in detail in chapter 7.8.4., is newer than the previously examined schemes. It has been set up by the Department of Electronics and Information Technology (DEITY) as part of Cyber Security Assurance initiatives of the Government of India. The purpose of the scheme is to evaluate and certify IT Security Products and Protection Profiles (PP) against the requirements of Common Criteria Standards at assurance levels EAL 1 through 4. The Certification Body is the STQC Directorate, Department of Electronics and Information Technology, Govt. of India.

7.8.4.4. SUMMARY

Common Criteria “delivers proof of quality and the reliability of the (security) product and offers the basis for the comparison of results of independent evaluations.” Starting from a few members, today the framework counts 17 Certificate Authorising Participants and 9 Certificate Consuming Participants, building trust in the quality of the evaluated security products and systems. Despite the harmonisation to a high extent of the common criteria schemes, differentiation in clauses like the ones mentioned above might have an impact on how appealing one scheme is to the interested parties which wish to be certified under the Common Criteria. Also transparency over the pricing is a factor of differentiation among the schemes. The Dutch scheme for example has published a pricelist on the website. Other scheme operators might inform on the price only in the form of a quote after a specific request. Finally, there are differences on the private/public nature of the Certification Body and the number of the Evaluation Facilities in each country.

The trust and confidence the Common Security framework adds to the evaluated products and systems can be regarded as one of its strengths. The transparency of the rules, certification schemes, certification owners and the criteria are strong elements of the Common Criteria and a good practice that needs to be followed. Trust is also urged by the quality of the criteria and processes: Common Criteria benefit from the accumulated expertise of experts from the par-

---

1020 Common Criteria Portal of India, Indian Common Criteria Certification Scheme (IC3S), no date. http://www.commoncriteria-india.gov.in/Pages/default.aspx
participant countries. The CC framework is flexible, designed to adapt to new challenges and best practices. Its structure also allows the organisations and other parties to specify the security functionality of a product and independently select the evaluation assurance level.

CC does not come without shortcomings and limitations. The main criticism are the following:

- Limitations of general evaluation methodology\(^{1022}\)
- Shortcomings in assessment of implementation and deployment vulnerabilities\(^{1023}\)
- Costly process in terms of money and time. The completion of the evaluation process is lengthy.\(^{1024}\) The certification time might in some cases exceed the lifecycle of a technology, for instance 1-2 years. Zhou et. al. also share the view that CC methodology and terminology are complex for developers to follow.\(^{1025}\)
- Point-in-time certification. The CC cover a particular version of the certified product or system in certain configurations. Changes to this version would not be covered by the certificate, which leads to two results; either the product or system needs to be recertified, which entails additional costs in time and money or the product is not recertified in order to cover the changes, and as a result only a version of the product or system is certified\(^{1026}\)
- The process is heavily weighted to addressing governmental security needs and expectations and as a result is difficult to be used for SMEs and simple systems.
- ECORYS also notes that there appears to be some degree of slippage in the use of CC evaluation procedures with certain countries pushing their own national testing regimes.\(^{1027}\)

Notwithstanding the shortcomings and the criticism to the CC, the CC framework is in general considered successful. The key elements of success can be outlined as follows:

- **Engagement of public and private sector**
  CC engage both governments, which are the signatory members and generally responsible for the implementation of the framework, and private testing facilities. The combination offers to the CC the reliability of the governmental participation and the flexibility of the private sector.


\(^{1024}\) Zhou, Changying and Stefano Ramacciotti, op. cit., p. 25

\(^{1025}\) Zhou, Changying and Stefano Ramacciotti, op. cit., p. 25


• Based on a technical standard
The norm of the scheme, the ISO/IEC 15408 standard, is a comprehensive standard, developed by experts in the field working in the public and private domain in the area of information security. Moreover, the hosting organisations, ISO and IEC, add to the validity and quality of the CC.

• Mutual recognition of certificates in participating countries worldwide
Key of the success is the mutual recognition of the certificates. Avoidance of duplication of evaluation process in the participating countries reduces the economic and human resources costs.

• Protection Profiles and Evaluation levels
Different protection levels apply to different technologies and environments. CC take into account that security risks and demands differ from product to product and system to system. As a result, the specific characteristics of a smart card related device or a biometric system are properly considered when developing the protection of the information system.

• Living documentation and updated procedures
The guidance from the Common Criteria Management Board and the possibility for National Interpretations, offer concise advice to the implementation of the CC. Updates of the framework, as the Collaborative Protection Profiles, facilitate the response of the CC to the new challenges and risks.

7.9. **CONCLUSION**

This chapter showed important and interesting security assessment approaches, requirements and guidelines, which are helpful for the further progress of the CRISP project and the development of its certification methodology.

The biggest impact on the CRISP project can probably be found in the ONVIF specifications and profiles, which offer important requirements for the interoperability of security products within a system. One shortcoming of the ONVIF – the missing of addressing possible freedom infringement implications of the security system – could be a possible point of improvement through our project. Here, we could for example also draw on the expertise of the EuroPriSe certification, which offers an excellent insight in the certification of privacy matters in security products and systems. The advantages of EuroPriSe can be found in the wide inclusion of data protection regulations and the transfer of these into a certification scheme for security products and systems, drawing on all aspects of the data processing and relying on legal requirements. Unfortunately here is the low implication of the privacy-certification scheme.

The international code of conduct for private security service providers can be included here, since they also have a strong connection to legal requirements, which they transfer on requirements for security services – although in a much broader perspective as is done in the EuroPriSe scheme. Which is also the biggest lack of the ICoC, the missing specifications and requirements for the special duties and task of security services – and which the code also probably doesn’t want to cover.

---

1028 Common Criteria, Protection Profiles, no date. website: https://www.commoncriteriaportal.org/pps/
1029 Common Criteria Collaborative Profiles, no date. https://www.commoncriteriaportal.org/pps/?cpp=1
Another interesting example was the Common Criteria certification scheme. It is a framework, which beyond its limitations and shortcomings, is considered successful and best practice, offering valuable lessons to other schemes and CRISP.

The remaining international security assessment solutions, mainly on supply chain and border security, but also on CBRNE security often have good insights in security/risk assessment tools, which are crucial for establishing security measures at the concerned facilities. Here especially the International Ship and Port Facility Security code offers a strong security assessment framework. Of the U.S. Customs and Border Protection programmes, especially the C-TPAT programme covers a large amount of minimum security requirements for supply chain & cargo transportation providers, from highway carriers, rail carriers over air carriers to sea carriers. Although the available requirements are again kept rather broad, the wide scope covers large parts of the supply chain security. To conclude with, the Common Criteria is a framework, which beyond its limitations and shortcomings, is considered successful and best practice, offers valuable lessons to other schemes and CRISP.

7.10. REFERENCES


Common Criteria, Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, v.3.1., rev. 4, September 2012


Common Criteria Management Committee, Mutual Recognition Agreement of Security Evaluation Certificates, v.3.0, January 2010


Indian Common Criteria Certification Scheme (IC3S), Quality Manual, issue 2, October 2012.


TUV Rheinland Nederland and Ministerie van Buitenlandse Zaken en Koninkrijksrelaties “Netherlands Scheme for Certification in the Area of IT Security (NSCIB), NSCIB Scheme Interpretation #1, Performing Site Audits”

TUV Rheinland Nederland and Ministerie van Buitenlandse Zaken en Koninkrijksrelaties “Netherlands Scheme for Certification in the Area of IT Security (NSCIB), NSCIB Scheme Interpretation #5 Addressing questions to the Certification Body”, version 2.1., July 1st, 2011


World Customs Organisation, “SAFE Framework of Standards to secure and facilitate global trade”, June 2012.


8. **ACREDITATION OF CERTIFICATION BODIES IN THE SECURITY FIELD**

8.1. **CURRENT STATE OF PLAY IN ACCREDITATION IN EUROPE**

8.1.1. **STANDARDS ON ACCREDITATION AND THEIR IMPLEMENTATION IN EUROPE**

ISO and the IEC\(^{1030}\) define accreditation as “third-party attestation related to a CAB conveying formal demonstration of its competence to carry out specific CA tasks”. This subchapter provides information on international standards which define the framework conditions for accreditation and European Regulation 765/2008 and presents relevant organisations in the accreditation landscape. The main guidelines for certification are given by ISO and the IEC at the international level. Figure 135134 gives an overview of the standards pertaining to CA and their scopes.

<table>
<thead>
<tr>
<th>ISO/IEC 17000:2004</th>
<th>Conformity assessment -- Vocabulary and general principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>This standard specifies general terms and definitions relating to CA, including the accreditation of CABs, and to the use of CA to facilitate trade. It does not provide a set of terms for all concepts that may be needed to describe particular CA activities. Terms and definitions are specified only where a defined concept would otherwise be incomprehensible or if an existing standard definition is not applicable. A description of the functional approach to CA is included in its Annex A.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ISO/IEC 17007</th>
<th>Conformity assessment – Guidance for drafting normative documents suitable for use for conformity assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>This standard provides principles and guidance for developing normative documents that contain specified requirements for objects of CA to fulfil and specified requirements for CA systems that can be employed when demonstrating whether an object of CA fulfils specified requirements. It is intended for use by standards developers not applying the ISO/IEC Directives, industry associations and consortia, purchasers, regulators, consumers and non-governmental organisations, accreditation bodies, CABs, CA scheme owners, and other interested parties, such as insurance organisations.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ISO/IEC 17011:2004</th>
<th>Conformity assessment – General requirements for accreditation bodies accrediting conformity assessment bodies</th>
</tr>
</thead>
<tbody>
<tr>
<td>This standard specifies general requirements for accreditation bodies assessing and accrediting CABs. It is also appropriate as a requirements document for the peer evaluation process for mutual recognition arrangements between accreditation bodies. Accreditation bodies operating in accordance with this standard do not have to offer accreditation to all types of CABs. For the purposes of this standard, CABs are organisations providing the following CA services: testing, inspection, management system certification, personnel certification, product certification and, in the context of this standard, calibration.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ISO/IEC 17030:2003</th>
<th>Conformity assessment – General requirements for third-party marks of conformity</th>
</tr>
</thead>
<tbody>
<tr>
<td>This standard provides general requirements for third-party marks of conformity, including their issue and use.</td>
<td></td>
</tr>
</tbody>
</table>


This standard specifies the general requirements for the peer assessment process to be carried out by agreement groups of accreditation bodies or CABs. It addresses the structure and operation of the agreement group insofar as they relate to the peer assessment process. The standard is not concerned with the wider issues of the arrangements for the formation, organisation and management of the agreement group, and does not cover how the group will use peer assessment in deciding membership of the group. Such matters, which could, for example, include a procedure for applicants to appeal against decisions of the agreement group, are outside its scope. The standard is applicable to peer assessment of CABs performing activities such as a) testing, b) product certification, c) inspection, d) management system certification (sometimes also called registration), and e) personnel certification. More than one type of activity can be included in a peer assessment process. This can be considered particularly appropriate when the body under assessment conducts combined assessments of multiple CA activities. The standard is also applicable to peer assessment among accreditation bodies, which is also known as peer evaluation.

ISO/IEC 17043:2010  Conformity assessment – General requirements for proficiency testing

This standard specifies general requirements for the competence of providers of proficiency testing schemes and for the development and operation of proficiency testing schemes. These requirements are intended to be general for all types of proficiency testing schemes, and they can be used as a basis for specific technical requirements for particular fields of application.

ISO/IEC 17065:2012  Conformity assessment – Requirements for bodies certifying products, processes and services

This standard contains requirements for the competence, consistent operation and impartiality of product, process and service CBs. CBs operating to this standard need not offer all types of certification. Certification of products, processes and services is a third-party CA activity (see ISO/IEC 17000:2004, definition 5.5). In this standard, the term “product” can be read as “process” or “service”, except in those instances where separate provisions are stated for “processes” or “services” (see Annex B of the document).


This standard describes the fundamentals of product certification and provides guidelines for understanding, developing, operating or maintaining certification schemes for products, processes and services. It is intended for use by all with an interest in product certification, and especially by certification scheme owners.


ISO/IEC TR 17026 provides an example of a type 5 product certification scheme for tangible products as described in ISO/IEC 17067.

---

1031 See Figure 136135 for a description.

This guide lays down methods of indicating conformity with standards and reference to in standards. While it is directed specifically to conformity with standards, it is recognised that it may be equally applicable to conformity with other technical specifications. It applies to indications of conformity made under the authority of a CB. The guide is primarily intended for International Standards but may also be used for national standards or other purposes.


This guide recommends good practices for all elements of CA, including normative documents, bodies, systems, schemes and results. It is intended for use by individuals and bodies who wish to provide, promote or use ethical and reliable CA services. These include, as appropriate, regulators, trade officials, calibration laboratories, testing laboratories, inspection bodies, product CBs, management system certification/registration bodies, personnel CBs, accreditation bodies, organisations providing declarations of conformity, designers and administrators of CA systems and schemes, and users of CA. The guide is designed to facilitate trade at the international, regional, national and sub-national levels.

Source: Standards presented in the figure
Figure 135: Overview of standards pertaining to conformity assessment and their scopes

ISO/IEC 17067:2013\(^{1032}\) provides specific information on the necessary elements of a certification scheme and the kinds of certification schemes. Twenty-one general elements of a certification scheme are defined:

- Scope
- Product requirements
- CA activities
- Certification requirements
- Requirements for CABs, for example accreditation and peer assessment
- CA methods and procedures
- Information supplied by clients
- Statement of conformity
- Mark of conformity
- Use of certificate and mark
- Resources for operating the scheme
- Reporting results of determination and surveillance activities
- Dealing with non-conformities
- Surveillance procedures
- Criteria for access to scheme
- Directory of certified products
- Contracts: owner, certification body (CB), client
- Conditions for certification: granting, withdrawing, etc.
- Clients’ complaints records, need for verification by CBs
- Clients’ reference to scheme in publicity material
- Records to be retained by scheme owner and CBs

It also describes eight major types of product certification schemes while noting that the elements in those systems can be combined in other ways to create additional systems. These eight types are presented in the following figure.

## D2.2: Consolidated report on security standards and certification

**CRISP project**

---

<table>
<thead>
<tr>
<th>Type PCS(^{1033})</th>
<th>Background</th>
<th>Examples of techniques used</th>
<th>Relevant information</th>
</tr>
</thead>
</table>
| Scheme type 1a      | Type test  | - samples requested by the CB  
                      - determination of the relevant product characteristics by testing (ISO/IEC 17025) or assessment  
                      - review of the test or assessment report  
                      - attestation of conformity | “Type approval” scheme, in which the samples may not be representative or statistically relevant for the entire product group. Attestation of conformity applies only to samples tested. |
| Scheme type 1b      | Batch test, including 100 percent testing | - samples requested by the CB  
                      - determination of the relevant product characteristics by testing (ISO/IEC 17025) or assessment  
                      - review of the test or assessment report  
                      - attestation of conformity  
                      - issue of a licence to use certificates or marks on the products | Attestation of conformity will relate to the whole population and a certificate of conformity for each product could be provided by the CB. |
| Scheme type 2*      | Type test plus periodic testing of products from the market | - samples requested by the CB  
                      - determination of the relevant product characteristics by testing (ISO/IEC 17025) or assessment  
                      - initial auditing of the production process or quality system  
                      - review of the test or assessment report  
                      - attestation of conformity  
                      - issue of a licence to use certificates or marks on the products  
                      - surveillance by CB taking samples from the market and testing or inspection to confirm ongoing conformity | Scheme may identify the impact of the distribution chain on conformity. When significant nonconformities are found, effective preventive measures may be limited since the product has already been distributed to the market. |
| Scheme type 3*      | Type test plus periodic testing of products from the point of production plus periodic assessment of the production process | - samples requested by the CB  
                      - determination of the relevant product characteristics by testing (ISO/IEC 17025) or assessment  
                      - initial auditing of the production process or quality system  
                      - review of the test or assessment report  
                      - attestation of conformity  
                      - issue of a licence to use certificates or marks on the products  
                      - surveillance by testing or inspection of samples from the factory and auditing of the production process | Scheme does not provide any indication of the impact the distribution channel plays on conformity. When serious nonconformities are found, the opportunity may exist to resolve them before widespread market distribution, depending on the frequency of surveillance. |

---

\(^{1033}\) Product certification schemes
**Scheme type 4**  
Type test plus periodic testing of products from the point of production and/or the market plus periodic assessment of the production process

- samples requested by the CB  
- determination of the relevant product characteristics by testing (ISO/IEC 17025) or assessment  
- initial auditing of the production process or quality system  
- review of the test or assessment report  
- attestation of conformity  
- issue of a licence to use certificates or marks on the products  
- surveillance by testing or inspection of samples from the factory and auditing of the production process  
- surveillance by testing or inspection of samples from the market

Scheme can both indicate the impact of the distribution channel on conformity and provide a pre-market mechanism to identify and resolve serious nonconformities.

**Scheme type 5**  
Type test plus periodic assessment of production process and/or audit of management system plus periodic testing of products from point of production and/or the market

- samples requested by the CB  
- determination of the relevant product characteristics by testing (ISO/IEC 17025) or assessment  
- initial auditing of the production process or quality system  
- review of the test or assessment report  
- attestation of conformity  
- issue of a licence to use certificates or marks on the products  
- surveillance of production process or quality system or both  
- surveillance by testing or inspection of samples from factory, open market or both

Scheme includes both testing and the assessment of that part of the quality system which relates to the conformity of the products with the specified requirements. This scheme provides significant flexibility for ongoing surveillance – quality system, factory samples and open market samples, as the last may be adjusted for a given situation.

**Scheme type 6**  
Covering certification of processes and services

- determination of the relevant product characteristics by testing (ISO/IEC 17025) or assessment  
- initial auditing of the production process or quality system  
- review of the test or assessment report  
- attestation of conformity  
- issue of a licence to use certificates or marks in relation to the process or service  
- surveillance by audits of the quality system  
- surveillance by assessments of the processes or services

Scheme is applicable to certification of services and processes. Initial and periodic assessment of service or process plus initial assessment and periodic auditing of management system.
<table>
<thead>
<tr>
<th>Scheme type n</th>
<th>Scheme indicates that scheme owner can select activities that suit the purpose of the scheme, in consultation with stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOTE:</td>
<td>*Scheme types 3, 4 and 5 require initial assessment of production process and/or management system</td>
</tr>
</tbody>
</table>

Source: Based on ISO/IEC 17067:2013
Figure 136: Overview of techniques used in major types of product certification schemes

The schemes described above represent some of the more common approaches to CA, but other combinations of techniques can be used according to the nature and purpose of the scheme.

A product certification scheme uses a set of rules, procedures and management techniques. If this is applied to more schemes, the common set of rules, procedures and management techniques are defined in a product certification system. A product certification system will only be defined if more than one scheme uses the same rules, procedures and management techniques. The schemes that are a part of a product certification system have a common framework, while each scheme varies in the application of the system and the specified requirements.

The following figure gives information on the adoption of the ISO/IEC accreditation standards of Figure 135134 as national standards in selected European countries.

As Figure 137136 shows, most of the CA standards have been adopted as national standards in many European countries. An exception to this is ISO/IEC TR 17026, which had only very recently been published at the time of writing this deliverable. National adoption of European standards often takes a few months or even up to a year, depending on national adoption procedures. At the time of writing this deliverable, it was unclear whether European countries other than the ones which had already adopted it (The Netherlands and Sweden) were in the process of adopting ISO/IEC TR 17026, were planning to start the process or had decided not to adopt it at all.

According to ISO and the IEC, there is insufficient attention paid at the international level to service and process certification.

---

8.1.2. EU Regulation 765/2008

Regulation 765/2008 sets out requirements for accreditation and market surveillance in Europe and specifies the legal framework for the European accreditation landscape. It promotes a uniform approach across Member States, in particular for products. To stop the demand for multiple documents to demonstrate the technical capacity of a CAB, it mainly requires the acceptance of only one accreditation certificate issued by a NAB of an EU Member State across Europe. Its main principles of accreditation are:

---

Accreditation is carried out by a single NAB appointed by its Member State (Article 4.1);
Accreditation is performed as a public authority activity (Article 4.5);
NABs operate free from commercial motivations (Article 8.1) and on a not-for-profit basis (Article 4.7); and
NABs do not compete with CABs or among each other (Articles 6.1 and 6.2).

Additional principles are:

- Stakeholder representation is ensured and
- Accreditation is the preferred means of demonstrating technical capacity in the regulated area.

Market surveillance is required to identify and remove dangerous products. Categorised under “dangerous” are:

- Products which could malfunction even if used as properly intended;
- Products which lack proper or any instruction; and
- Products where either the CE logo has been misused or the CE logo is fake.

In cases of serious risk, immediate and preventive actions are required. This regulation defines that the CE logo is the only logo which shows conformity with harmonised Community regulations. Other logos may be applied to products if they provide additional information, value or cover a domain outside the Community regulations. This also shows potential for the establishment of an EU security mark.

**General principles for national accreditation bodies**

The Regulation includes general principles and requirements for NABs. These requirements are in line with the requirements of the relevant ISO/IEC standards, although some of them can be perceived as being more rigorous, in particular the principles shown before based on Articles 4 and 6.

In order to meet the requirements of the Regulation, Member States had to change their national accreditation systems. Several Member States only had to make minor changes, but others had to substantially overhaul their system. All Member States had set up NABs, as had EFTA countries and Turkey. In some cases, this meant that they had to merge several accreditation bodies. The following sections take a closer look at selected specific accreditation issues.

---

1038 See Articles 4, 6 and 8 of the Regulation.
Peer evaluation

Peer evaluation is regarded to be the most essential measure to ensure that the European accreditation system ensures a high quality of conformity assessment in Europe. Such peer evaluation is the key prerequisite for the mutual recognition of accreditation certificates, which is described in more detail later. According to the European Commission, the current objectives are to further strengthen this evaluation process, to enhance the availability of appropriate peer evaluators and to further harmonise approaches, particularly in regulated market areas.

Market surveillance by Member States

Regulation 765/2008 includes specific requirements for the organisation of market surveillance. Member States must establish, implement and update their market surveillance programmes. They must also communicate the programmes to other Member States and to the Commission and make them accessible to the public via the internet. Most Member States have implemented specific solutions to ensure the fulfilment of these requirements. Their replies to a questionnaire on these issues can be summarised as follows:

- **Responsibility and identity of authorities**: Most Member States only needed to make some small adjustments to pre-existing market surveillance activities (for example establishing a programme for the enhancement of market surveillance).

- **Communication and coordination mechanisms between market surveillance authorities** varies among Member States: communication channels are sometimes based on an informal agreement, or communication takes place via specific coordination bodies, working groups or market surveillance committees.

- **Procedure to follow up complaints**: Although most Member States had already set up systems for complaints, the majority indicate that these can be further improved.

The European Commission discovered that some Member States placed more emphasis on information concerning the general organisation of market surveillance, while others focused on information on sector activities. Therefore the approaches to provide relevant information need more harmonisation.

Cross-border accreditation

With three exceptions, Article 7.1 of the Regulation requires that CABs seek accreditation in the Member State where they are established. The exceptions are where:

---


1040 European Commission, op. cit., 2013c.

1041 European Commission, op. cit., 2013b.

1042 European Commission, op. cit., 2013b.
The Member State in question has not set up an NAB;
- The NAB does not perform accreditation for the activity for which accreditation is sought; or
- The relevant NAB has not successfully undergone peer evaluation.

So far, the first scenario had not become an issue, as all Member States have set up an NAB. The other two scenarios are more relevant, however, as not all NABs perform the full scope of activities.\(^\text{1043}\)

Based on these clearly defined framework conditions, solutions are needed for multinational CABs where the head office is in one Member State and activities are exercised in another or several Member States. The TÜV provide important examples for such CABs in the security context.

The accredited CA results given on the basis of free provision of service must be recognised by the public authorities and accepted on the basis of the mutual recognition principle set out in Article 11(2) of the Regulation: “National authorities shall recognise the equivalence of the services delivered by those accreditation bodies which have successfully undergone peer evaluation under Article 10, and thereby accept […] the accreditation certificates of those bodies and the attestations issued by the conformity assessment bodies accredited by them.”

Based on Article 7, a solution regarding the accreditation of multinational CABs was needed. The key question was: “Can the operations of the local entity be covered by the accreditation of the head office issued by the NAB where the head office is established or shall the local entity be accredited by the local NAB?”

Article 7 was perceived to be very stringent and unnecessarily burdensome in this regard. The risk of suffering a competitive disadvantage compared to third country organisations was feared.\(^\text{1044}\) Should a strict interpretation of this article be applied, multinational CABs may not benefit from the advantage of one accreditation certificate for the EU, despite avoiding multiple accreditations being one of the objectives of the Regulation.

The majority of multinational CABs had their local entities accredited by local NABs for a long time. This resulted in multiple accreditations from various NABs. Based on the mutual recognition principle provided by Article 11.2 of the Regulation, regional demand for re-accreditation was no longer deemed acceptable. As a solution, the European Commission demanded that\(^\text{1045}\) “duplication of unnecessary assessments and burdens on multinational CABs should be avoided”. In addition, it was highlighted that adequate controls of local entities of multinational CABs must be assured.

\(^\text{1043}\) European Commission, op. cit., 2013b.
\(^\text{1044}\) According to the European Commission, op. cit., 2013a, the Regulation does not apply to CABs from third countries, which are therefore free to request accreditation with the European NABs of their own choice.
\(^\text{1045}\) European Commission, op. cit. 2013a, p. 9.
Notification without accreditation

The regulation prefers accreditation as a means for demonstrating the technical competence of a CAB for the purposes of “notification” under specific legislation. In this context, “notification” is defined as acknowledging the body’s ability to assess product compliance with the requirements of a given regulation or directive. Again, here the European Commission\textsuperscript{1046} only refers to products, not to systems or services.

As a solution for several specific issues, Article 5.2 provides a framework for notification without accreditation: Member States notify the Commission and other Member States of those CABs they want to authorise to carry out specific CA tasks based on specific technical legislation. By deciding which bodies to notify, Member States have the final responsibility for the technical competence and independence of such bodies, but they must verify these organisations based an adequate assessment process.\textsuperscript{1047}

When a Member State decides to use an alternative assessment method and not to base its notification on accreditation, according to Article 5.2 of the Regulation, “it shall provide the Commission and the other Member States with all the documentary evidence necessary for the verification of the competence of the conformity assessment bodies it selects for the implementation of the Community harmonisation legislation in question”.\textsuperscript{1048}

In order to ensure the necessary level of confidence in the competence of CABs and in the issued test reports and certificates, national authorities should give detailed and comprehensive information by describing how the candidate for a notified body is being assessed as qualified to carry out the tasks for which it is notified and showing that it fulfils the applicable criteria relating to notified bodies. This information linked to a given notification is made available through the NANDO tool to the Commission and other Member States. The alternative evaluation procedure should include the following elements:

- Candidates for a notified body should be made aware of general conditions, their rights and obligations, and requirements relating to the assessment carried out in view of notification;
- The existence of a formal application procedure;
- An assessment process for applicable requirements, which should consist of a) a review of documents and b) an on-site assessment to check technical and procedural aspects;
- Production of an assessment report;
- A decision-making process;
- The existence of systematic surveillance and a related sanction mechanism provided for periodic surveillance; and
- A demonstration of the national authorities’ own technical competence for assessing CABs for the purposes of notification under technical harmonisation legislation.\textsuperscript{1049}

\textsuperscript{1046} European Commission, op. cit., 2013b.
\textsuperscript{1048} European Commission, op. cit., 2013a, p. 14
\textsuperscript{1049} European Commission, op. cit., 2013a, p. 15
When choosing the alternative assessment process instead of formal accreditation, national authorities should indicate the reasons why accreditation is not chosen to back up the notification process.

The use of accreditation for notification purposes differs between Member States and between sectors. In some Member States, accreditation is compulsory for notification, while others apply a rather mixed approach. Recent statistics reveal that 3,106 notifications had been granted since the introduction of the Regulation until June 2012, 2,196 of them being accredited.\textsuperscript{1050} Accreditation is thus becoming a frequently used instrument for notification. Nevertheless, closer communication between national authorities and accreditation bodies is still desirable.

\section*{8.1.3. The European Accreditation Framework – History and Future Plans}

According to Article 14 of Regulation (EC) 765/2008, the Commission recognised the European Cooperation for Accreditation (EA) as the European accreditation infrastructure\textsuperscript{1051}. It is regarded as “an organisation of major European interest, similar to the European Standardisation Organisations (CEN, CENELC and ETSI) in the field of the European standardisation policy”.\textsuperscript{1052} European NABs fulfilling the requirements of the Regulation are almost automatically members of the EA (Article 4.10).\textsuperscript{1053} The EA Multilateral Agreement (EA MLA) is an important document in this regard. It is a signed agreement between the EA’s Full Members in which the signatories recognise and accept both the equivalence of the accreditation systems of other members and the reliability of the conformity assessment results provided by CABs accredited by all signatories.\textsuperscript{1054}

In 2009, the European Commission, EFTA, EU Member States and the EA signed an agreement to work closely together on a successful implementation of the accreditation chapter of Regulation 765/2008.\textsuperscript{1055} In addition, in 2010 the Commission and the EA signed a framework partnership agreement for the 2010–2014 period. This agreement allows financial support for the EA’s services as envisaged by the Regulation. The relevant EA activities include:

- Technical work linked to the peer evaluation system;
- Informing interested parties and participation in international accreditation activities;
- Drawing up and updating contributions to guidelines relating to accreditation, notification of CABs, conformity assessment and market surveillance; and
- Activities of assistance to third countries.\textsuperscript{1056}

\textsuperscript{1050} European Commission, op. cit., 2013b, p. 5
\textsuperscript{1051} See Article 14 of the Regulation.
\textsuperscript{1052} European Commission, op. cit., 2013a, p. 12.
\textsuperscript{1053} European Commission, op. cit. 2013a.
\textsuperscript{1056} See Article 32 of the Regulation.
Furthermore, the EA has been working on a common understanding on how to perform accreditation and also on supporting accreditation in the relevant regulated sectors. This has already resulted in a number of guidance documents.\(^{1057}\)

According to a report by the European Commission,\(^{1058}\) the cooperation with the EA has been very successful. The report argues that the progress made so far should be consolidated to enhance accreditation’s role as the last control level within the European conformity assessment system.

The EA enjoys worldwide acceptance and its members also include a number of non-European accreditation organisations as associate partners, for example those from Israel, Jordan and Morocco.\(^{1059}\)

A contract between the European Commission and the EA specifies the latter’s work between 2014 and 2017. A key component is a draft EA plan for the relevant period.\(^{1060}\) This includes the management of a rigorous peer evaluation system operating on the basis of sound and transparent evaluation criteria and procedures. The main elements of the plan are:\(^{1061}\)

- Consolidate the function of the EA as the European accreditation infrastructure;
- Strengthen and improve the peer evaluation process and activities;
- Further harmonisation of the criteria for Notified Bodies;
- Enhanced servicing the Commission as a technical resource in development, maintenance and implementation of accreditation and conformity assessment in the Community;
- Give support to the private sector with respect to accreditation and conformity assessment schemes; and
- Consolidate the status of the EA at the international level and strive to implement European policy and principles for accreditation as the last international level of control.

At the international level, cooperation between the EA and its members and other accreditation bodies takes place within two organisations:

- The International Accreditation Forum (IAF), facilitating cooperation between accreditation bodies accrediting certification and inspection bodies, and
- The International Laboratory Accreditation Cooperation (ILAC), operating between accreditation bodies accrediting laboratories and inspection bodies.

The framework conditions of the international accreditation framework will be described in a separate sub-chapter.

---


\(^{1058}\) European Commission, op. cit., 2013b.

\(^{1059}\) DAKK5, “EA-Mitgliederzahl steigt weiter an” 22.06.2012. [http://www.dakks.de/content/ea-mitgliederzahl-steigt-weiter](http://www.dakks.de/content/ea-mitgliederzahl-steigt-weiter);


\(^{1061}\) European Commission, op. cit., 2013c.
8.1.4. **PRINCIPLES OF THE EUROPEAN COOPERATION FOR ACCREDITATION**

8.1.4.1. **BASIC REQUIREMENTS ACCORDING TO ISO AND THE IEC**

According to the EA, SOs should follow ISO/IEC 17007 as a general guide when designing normative documents for conformity assessment. In addition, ISO/IEC 17067 provides guidelines for developing and managing certification schemes. These pertain to:

- Scheme owners (clause 6.3);
- Scheme development (clause 6.4);
- The content of a scheme (clause 6.5);
- Maintenance and improvement of a scheme (clause 6.6); and
- Scheme documentation (clause 6.7).

These guidelines should be applied by SOs establishing certification schemes for products, processes and services. The requirements for establishing certification schemes for the certification of persons are contained in clause 8 of ISO/IEC 17024.

8.1.4.2. **SPECIFIC EA REQUIREMENTS ON CONFORMITY ASSESSMENT SCHEMES**

In line with key ISO/IEC documents, the EA highlights the typical elements of a conformity assessment scheme in its document EA-1/22 as:

- Selection of the object(s) of conformity assessment by selecting specified requirements to be assessed and planning information collection and sampling activities;
- Determination, including the use of one or more determination methods (e.g. tests, audits and/or examinations) to develop complete information regarding fulfilment of the specified requirements by the object of the conformity assessment or a sample thereof;
- Review and attestation, including the review of evidence from the determination stage, and a subsequent attestation that the object of conformity assessment has been reliably demonstrated to fulfil the specified requirements, and any subsequent marking or licensing and related controls, where applicable; and
- Surveillance (if needed), including the frequency and extent of surveillance activities and reassessments to ensure the object of conformity assessment continues to fulfil the specified requirements.

Additional elements of certification schemes include:

- The object of certification: management systems, or products, services and processes, or persons (i.e. their expertise or competence);
- Requirements against which the object of certification shall be assessed and certified. These requirements may be international standards, or standards or specifications set out within the sector, or specifications of a group of manufacturers;

---

• Description of the certification system; and
• Requirements applicable to CABs which are supplementary to the international standards for CABs.\(^{1063}\)

The Annex of EA-1/22 lays down the guidance to be considered by an SO when designing a CAS in order to facilitate acceptance by EA members. It reflects the contents of the relevant ISO/CASCO standards and guides.

8.1.4.3. **Topics for the validation of certification schemes**

The EA provides guidance for the validation of certification schemes, which covers nine areas: \(^{1064}\)

1. **Object**
   a) What is the object of certification?
   b) Which (group of) PSS etc. does the conformity assessment scheme cover?
   c) What aspect of the PSS etc. does the statement of conformity relate to?

2. **Certificate**
   a) What is the conformity statement which appears on certificates?
   b) What are the validity conditions of the certificate or the statement of conformity?
   c) How is the applicable certification system stated or referred to?

3. **Certification mark**
   a) How is the significance of the certification mark communicated to the market?
   b) Is there any significant risk of the certification mark being misinterpreted or misused?

4. **Certification requirements**
   a) Identify the scheme documents where the requirements are stated.
   b) How is it demonstrated that the requirements are possible to evaluate?
   c) Are legal requirements included?
   d) Does the scheme only contain legal requirements?
   e) How is compliance with legal requirements determined?
   f) Are there documents explaining or interpreting the requirements?
   g) Have the documents of 4f been published?
   h) Who are the authors of the interpretation document(s)?

\(^{1063}\) EA, op. cit., 2014, p. 16.
\(^{1064}\) EA, op. cit., 2014, pp. 16ff.
5. Certification system
a) Which evaluation method is used in order to determine conformity?
b) How does the SO/CAB demonstrate that the method is suitable for supporting the conformity statement?
c) Which method does the SO/CAB rely on to monitor that the certificate holder continues to comply with requirements?
d) How does the SO/CAB demonstrate the suitability of the method in order to monitor that the certificate holder continues to comply with requirements?

6. Conditions
a) Which criteria are required for granting, maintaining, expanding, reducing, extending, suspending or revoking certification?
b) Is the definition of non-conformity in line with the competence standards for CABs and/or IAF guidance?
c) What rights and obligations are stipulated for the SO, CBs and applicants?
d) What records are kept demonstrating continued compliance with the requirements?
e) What are the arrangements relating to registration of complaints by certificate holders?

7. Procedures
a) Are the certification procedures described, and if so, where is the description to be found?
b) Has the suitability of the procedures been demonstrated?

8. Expertise
a) Are there competency requirements for certification auditors?
b) Are there competency requirements for decision-makers?
c) Are there competency requirements for other staff members?
d) How has it been substantiated that the competency requirements are appropriate?

9. Public nature
a) Where are the scheme documents published?
b) Have these documents been made public?
c) Does the SO have any market surveillance, for example lists of certified products, services, etc.?

While item 4f regarding the publication of certification requirements may be difficult in the security context (and would contradict ECAC principles, for example), items 4c and 4e provide interesting input for further CRISP activities, for example in WP 4.
8.1.4.4. **Acceptance of Assessment Schemes by European Accreditation Bodies**

Based on the principles outlined in previous sections, the acceptance of a CAS by an EA member requires: 1065

- The identification of the most suitable standard to be used to assess the competence of the CABs participating in the conformity assessment scheme;
- The use of this standard as the reference for the accreditation of CABs; and
- That the CAS and the SO meet the requirements laid down in the EA-1/22 document.

Nevertheless, EA members’ acceptance of a given CA scheme does not represent a judgment on the technical robustness, market value or usefulness of the technical requirements thereof.

8.1.4.5. **Duties of Scheme Owners**

The EA highlights the difference between scheme owners (SOs) and CABs and defines specific guidelines for the relationship of the different parties.

The SO shall be able to demonstrate market support for the CA scheme by relevant interested parties. In particular, the viewpoint of parties representing the CA scheme end-users (e.g., consumers or industry) is important. The SO shall also show that the CA scheme has been validated based on the documentation of the following aspects:

- A description of the purpose of the scheme;
- A description of the requirements of the scheme;
- An analysis of the appropriateness of the established requirements for fulfilling the defined purpose of the scheme;
- A description of the methods to be used for determining fulfilment of the requirements;
- An analysis of the appropriateness of the described methods to be used for determining fulfilment of the requirements;
- A decision on the CA activity to be used (including the identification of the applicable CA standard); and
- An analysis of the appropriateness of the selected CA activity. 1066

The SO shall ensure that only accredited CABs with whom agreements have been closed use the scheme. Such agreements must guarantee that the CAB will use the scheme without limitations or additions.

The SO shall be responsible for keeping all active NABs and CABs informed of relevant information and developments relating to the CAS, in particular proposed changes in requirements.

---

8.1.4.6. **MULTINATIONAL CASs**

Regarding the implementation of multinational CA schemes, the EA defined specific processes. Before starting an evaluation of a multinational CA scheme, an NAB shall inform the EA Secretariat that it has been approached by the SO to perform the initial evaluation. Once the home accreditation body (hAB) has performed the initial evaluation of a CA scheme, it shall report the outcome thereof to the EA Secretariat. The EA Secretariat will inform all EA members that a new CA scheme is under evaluation and circulate the CA scheme documents and hAB evaluation report, which can then be commented on by the EA members within 30 days of their distribution.\(^{1067}\)

8.1.5. **SPECIFICS IN THE SECURITY FIELD**

In the security field, specific additional accreditation applies in Europe (and also in other countries such as the U.S.). In many cases governmental agencies are entrusted with specific duties. An example is provided by Common Criteria, which was described in the previous chapter. In Sweden, for example, ČSEC (Sveriges Certifieringsorgan för IT-Säkerhet) at FMV is responsible for the accreditation of Common Criteria certification providers. Försvarets Materielverk (FMV) is a civil authority under the Swedish Ministry of Defence.\(^{1068}\)

In Germany, the Bundesamt für Informationssicherheit, which is accredited by the German accreditation body DAkkS, accredits providers of Common Criteria certification services.


8.2. IMPLEMENTATION OF REGULATION 765/2008 IN SELECTED EUROPEAN COUNTRIES

8.2.1. FRANCE

The Comité français d'accréditation (hereinafter COFRAC) is the national accreditation body in France. It was created as a non-profit organisation in 1994 under the Act of 1 July 1901. The Act for Economic Modernisation of 4 August 2008 and its implementing regulation of 19 December 2008 designated COFRAC as the sole national body authorised to issue accreditation certificates to CA entities in France, in accordance with Regulation 765/2008 of the European Parliament and of the Council, whatever the sector concerned. A first insight regarding the structure, composition and activities of this organisation was presented in Section 3.3.4 of this deliverable; this section seeks to go further.

The most outstanding feature of COFRAC is that all interested parties such as: accredited agencies or their representative groups; business professional groups or buyers and users of the agencies; public interest representatives (government, state agencies, national institutes, consumer associations or final users) are represented in a balanced way within its governing bodies (the Board of Administrators and Section Committees).

This broad representation contributes to COFRAC’s high level of international recognition and confidence among partners, government and end-users in the field of CA. COFRAC is structured in four sections to manage accreditations:

- Section 1: Laboratories divided into Biology/Biochemistry, Chemistry and Environment, Mechanics, Physics, and Electrical Inspection;
- Section 2: Inspection;
- Section 3: Certifications; and
- Section 4: Human Health.

By 31 December 2013 COFRAC had delivered over 2,800 accreditations in all sectors (68 percent in the Laboratory Section, 17 percent in the Inspection Section, 10 percent in the Human Health Section and 5 percent in the Certifications Section). By the end of 2014, COFRAC had delivered over 3,000 accreditations in all sections. The share of the Certifications Section increased slightly in the number of accredited entities last year due to ad hoc requests for new domains (cathodic protection, information systems, etc.).

Although accreditation is a voluntary activity, it is usually developed within a statutory framework. It is then required by public authorities as a preliminary to future approval for the application of a national regulation, or with a view to notification within the framework of a European Directive. This trend towards recourse to accreditation as a prerequisite to notification has grown since the publication of the European regulation of 9 July 2008 on accreditation and market surveillance. The ultimate aim of an accreditation procedure is to establish trust in the service provisions fulfilled. Accreditation is required to represent the ultimate level of control of CA activities in terms of technical competence. Several requirements expressed in the standard ISO/IEC 17001 aim to achieve confidence in accreditation bodies (independence, impartiality, transparency and competence).
Regarding the role of standards in the accreditation context, three levels – accreditation, CABs and companies employing the services of accredited entities – can be singled out, as shown in Figure 138.

Source: COFRAC
Figure 138: Accreditation and certification in France
The accreditation process

The accreditation process in COFRAC follows a strict four-step procedure. A number of important procedures have to be successfully passed before a final decision is delivered. The process leading to accreditation is as follows:

1st step: Preliminary analysis of the application. After the receipt of the formal request, COFRAC considers the admissibility of the case. If the analysis is positive, an agreement between the applicant and COFRAC is established.

2nd step: Evaluation. Every accreditation must be defined by an evaluation programme which is conducted by a suitable evaluation team. The assessments are steered by COFRAC-qualified experts who are proficient in all aspects of the evaluation. Their methodology is based on a combination of rigor in selected procedures and evaluation methods and control systems and of flexibility afforded by a pragmatic approach which takes into account the particularities of each body applying for accreditation.

3rd step: Decision. The team evaluation is examined by a committee. The final opinion is based not only in regulations but also in rules and codes of practice. Subsequently, the standard shall guarantee high recognition and acceptance of COFRAC’s decisions.

4th step: Issuing of accreditation. The director of COFRAC notifies the applicant of the decision. With regard to scope, accreditation is not necessarily issued for an entity’s full range of activities. It is obtained for a specific field or competences related to the accreditation, or the application, and is limited to particular geographical locations. Regarding the duration, the accreditation is issued for a defined period. The maximum first period is four years, during which regular assessments will take place. A new revision has to be followed after this period and the renewed accreditation is valid for a period of five years.

ISO Standards and guides used by COFRAC for granting accreditation are shown in Figure 137/136 and Figure 143. Additional relevant documents are EMAS, ISO 14065 and Regulation (EU) No. 600/2012 and, for bodies responsible for the qualification of companies (NF X 50-091).

Regarding certification, the document Règlement d’Accréditation CER REF 05 aims to present the process and the rules for evaluation and accreditation of the agencies listed in its scope, and clarifies the rights and obligations of these entities or accredited candidates. The scope of the regulation is for bodies carrying out the following activities: CBs for products, services and processes/management and technical qualification systems in companies; Personnel certifications bodies; Bodies responsible for the qualification of companies; Bodies responsible for checking environmental statements and; Bodies responsible for checking statements on greenhouse gas emissions.

The provisions of the above-mentioned document have been applicable since 1 January 2015 by the bodies involved in evaluation and accreditation processes and by organisations accredited or applying for accreditation.

Along with the above-mentioned Règlement CER REF 05 and in the context of security certification, COFRAC implements:
The IAF Guide for the application of the ISO/IEC 65 Guide and some reference documents such as specific requirements for accreditation of CBs of industrial products by type testing in accordance to NF EN 45011;

Specific requirements for the qualification of security audit providers of information systems (CERT CPS REF 33);

Specific requirements for accreditation of training organisations for CBs of competent persons in radio-protection (CERT CPS REF 34); and

Specific requirements for accreditation of CBs for providers of localisation networks (CERT CPS REF 38).

Règlement d’Accréditation INS REF 05 presents the process for the accreditation of inspection bodies and is complemented by the INS REF 02 requirements for the accreditation of inspection bodies, which establishes the requirements for accreditation of inspection bodies according to the standard EN ISO/IEC 17020:2012. Finally, Règlement d’Accréditation LAB REF 05 has the purpose of regulating the accreditation process for laboratories and is complemented by the LAB REF 02 requirements for the accreditation of laboratories, which establishes the requirements for laboratories’ accreditation according to the standard EN ISO/IEC 17025.

COFRAC publishes very interesting information on accreditation in several areas in the form of COFRAC worksheets (Fiches COFRAC). The most important of these from the point of view of CRISP are on:

1. **Accreditations in the field of energy security:**

the accreditations delivered by COFRAC in the field of energy security target public and industrial policies on: security of production and supply of energy and safety, quality and performance of the energy distribution. For each of these policies, the use of accreditation (mandatory or voluntary) or the projected developments can be distinguished according to their purposes.

   a) *Safety production and energy supply (transportation of high-voltage electrical energy, oil and gas)*

   - Accreditations to certify the competence of the bodies responsible for making inspections or testing energy facilities (or components of facilities) at risk.
     - Voluntary accreditation for inspections of the factory manufacturing and assembly of structures, equipment and materials for basic nuclear installations (INB).
     - Voluntary accreditation for the control of the implementation of basic nuclear installations (INB) regulatory operations for maintenance and monitoring of Nuclear Facilities Under Pressure (ESPN).
     - Mandatory accreditation for the control of the commissioning of fuel gas transmission pipelines and liquid or liquefied hydrocarbons.
     - Mandatory accreditation for service monitoring of cathodic protection of gas transmission networks (on steel).
     - Voluntary accreditation for the tests to be conducted on material intended to equip the high and medium voltage aerial installations.
Voluntary accreditation for technical inspection of the construction and operation of the public electricity networks and direct power lines.

Accreditation to verify the ability of companies to ensure the safety of workers involved in hazardous environments working in energy installations.

b) Safety, quality and performance of the energy distribution

Volunteer accreditations to enhance the competence of laboratories assessing energy products or materials used in energy distribution.

- Accreditation for testing to be conducted on oil products and liquid or gaseous fuels to certify the composition and characteristics.
- Accreditation for testing to be performed on hardware (cables and accessories) intended to equip the low voltage aerial installations.
- Accreditation for testing to be carried to the construction and during type approval of electrical meters and current transformers.
- Accreditation for testing to be performed on measurement equipment of flow fuel gas or hydrocarbons.

Accreditations in order to certify the competence of the bodies responsible for carrying out security checks on power distribution facilities.

- Mandatory accreditation prior to the issuance of the approval of MEDDE ( Ministère de l'Ecologie, du Développement Durable et de l'Energie) for tightness control of underground flammable liquid tanks and associated equipment.
- Mandatory accreditation prior to the issuance of the approval of MEDDE for periodic inspection ICPE (installation classified for environmental protection) subject to declaration (sections relating to the storage and distribution of gas, oil and flammable liquids).
- Mandatory accreditation for service monitoring of cathodic protection of gas distribution networks in steel.
- Voluntary accreditation for the control of public facilities meter before gas (distribution point)

Accreditation to verify the qualification of stakeholders on energy distribution facilities.

2. Accreditations in the field of industrial risks and damages:

- Industrial safety materials and equipment including for the transport of dangerous goods: equipment under pressure; explosives; protection systems to be used in explosive atmospheres; inflammable liquids and petrol liquids;
- Technological risks and pollution: control of containers and tanks for transport of dangerous goods; development of accreditation for internal inspection of pressure equipment;
- Prevention of pollution and environmental quality.
8.2.2. Germany

Germany’s national accreditation body is DAkkS, the Deutsche Akkreditierungsstelle GmbH. Based on EU Regulation 765/2008, the Accreditation Body Act (AkkStelleG), and international standards and agreements, it has been the sole national accreditation body in Germany since January 2010. The regulatory framework of its work also includes the Regulation on the Entrustment of the Accreditation Body (AkkStelleGBV) for the transfer of public authority duties to the accreditation body, the Regulation on Costs of Activities of the Accreditation Body (AkkStelleKostV) for determining the fees for the accreditation body, and the Regulation on the Accreditation Symbol (SymbolVO) for the design and use of the accreditation symbol. Figure 139138 presents its structure and duties.

According to DAkkS, security issues, which are relevant for CRISP, are coordinated by Division 2: Product and Installation Safety – Telecommunication – EMC. In addition, Division 1, which is responsible for general duties, includes departments for construction, fire protection and for air transport. Division 6 is responsible for systems of certification and verification. It has six departments, including those for health and safety and information technology.

The DAkkS accreditation process consists of four stages: Application, Assessment, Accreditation and Surveillance (see Figure 140139).

Application
The accreditation process for a CAB begins by posting an application to the Central Application Processing (ZAB) of DAkkS. The ZAB reviews the application in coordination with the DAkkS division in charge. This procedure also includes a review of whether a notifying authority must be included in the accreditation procedure. After passing a successful review of the application, DAkkS informs the applicant about the next steps.

Assessment
During the second phase of the accreditation procedure, DAkkS assesses the technical competence and management system of the CAB with a team of assessors. The experts initially review the submitted documents, followed by a site visit on an agreed date. The results are documented in an assessment report. Irregularities noted in the report may be rectified by the client by implementing the relevant corrective measures within two months of the assessment date. The specific CAB is then subjected to another review and assessment.

---

1069 The Accreditation Body Act (AkkStelleG) of 31 July 2009 describes the implementation of the requirements of Regulation (EC) No. 765/2008 in Germany. The act defines tasks and responsibilities of the accreditation body, the organisational form of the accreditation body; the accreditation advisory board, the accreditation symbol, fees and disbursements, entrustment, supervision, cooperation with public authorities, and transfer of existing surveillance obligations (DAkkS, Accreditation Body Act (AkkStelleG), no date, http://www.dakks.de/en/content/accreditation-body-act-akkstelleg).
Source: DAkkS

Figure 139: Divisions of Germany’s DAkkS

Source: Based on a figure from DAkkS

Figure 140: The accreditation process at DAkkS

---

1073 This picture is provided by DAkkS at http://www.dakks.de/sites/default/files/sharedpics/Orga/dakks-organigramm20140505_1000px_web_en.jpg.

Accreditation
In the third phase, an accreditation committee (AkA) evaluates the assessment results and decides on whether the accreditation should be granted. DAkkS certifies the successful completion of the accreditation phase with an accreditation certificate. This means that DAkkS provides the inspected organisations with attestation that the audited assessment services conform to the relevant standards or laws and hence attests to the technical competence of the bodies. The certificate is subsequently included in the database of the accredited bodies. DAkkS then issues an accreditation symbol, the seal of approval for competent CAs, as shown in Figure 141.

Source: DAkkS
Figure 141: Example of the DAkkS accreditation symbol with unique registration number

Upon request, DAkkS allows accredited bodies to use its accreditation symbol.

Surveillance
In general, accreditations are valid for five years, though several factors can lead to a revocation of accreditation notification by DAkkS, including:

- Non-compliance to essential accreditation requirements (e.g. personnel, facilities or premises);
- Repeated or very serious infringement of accreditation rules;
- Deliberate deception on the part of the accreditation body by providing incorrect or incomplete information which is essential for the assessment of the CAB; and
- Non-compliance with regulations issued even after setting a grace period.

During the accreditation period, DAkkS conducts two to three surveillances at fixed intervals, depending on the kind of CAB. The document “Allgemeine Regeln zur Akkreditierung von Konformitätsbewertungsstellen” specifies reasons for withdrawing an accreditation according to Article 5.4 of Regulation 765/2008 and §§48ff. of the German Verwaltungsverfahrensgesetz (VwVfG). The accreditation cycle ends after five years at the latest, with the expiry of the accreditation or re-accreditation.

In addition to the accreditation of CABs, DAkkS also accredits CA programmes. Its procedure for the admission of new CA programmes consists of 13 steps:

---

1. Estimation of the need for and the benefits of the new programme and the number of expected applications for accreditation by the DAkkS;
2. Integration of competent authorities;
3. Examination of the accreditation potential with the involvement of the relevant sector committees;
4. Basic decision to launch the new CA programme by DAkkS;
5. Informing the applicant of the decision and publication on the DAkkS website;
6. If necessary, participation in national and/or international bodies regarding the accreditation of bodies for the new programme;
7. If necessary, establishment of a sector committee to provide the required technical accreditation and assessment rules or integration in an existing sector committee
8. Development/determination of the applicable rules involving the sector committees etc.;
9. Developing a pool of expert reviewers for the new programme (if necessary);
10. Training of staff and assessors;
11. If necessary, introduction of new AkA members for the new assessment programme;
12. Final decision by DAkkS to launch the new programme, including decisions on organisational/structural measures;
13. Integration of the programme in the activity of the DAkkS.

The development of CA programmes has to be conform to the standard ISO/IEC 17007, especially Chapters 4 to 6. In addition, DAkkS formulated nine specific requirements.\(^\text{1077}\)

1. Consistent with the EA (2014),\(^\text{1078}\) the SO has to identify interested parties and analyse their needs. These have to be involved in the development of the programme.
2. The SO shall also be able to demonstrate market support for the CAS.
3. The programme is to be developed by competent persons. Their competence must include skills and knowledge pertaining to CA procedures.
4. The programme needs to be validated. The following questions are relevant in this context:
   - Is the CA practicable?
   - Is the CA measurable?
   - Do the programme requirements ensure reproducible and reliable results?
5. The programmes must follow the rules of the respective standard (e.g. DIN EN ISO/IEC 17020, 17024 or 17065).
6. The requirements of DIN EN ISO/IEC 17011 must be met.
7. Additional requirements must not contradict Regulation 765/2008, DIN EN ISO/IEC 17011, or the rules of the EA, ILAC, IAF or DAkkS. The assessment must be efficient.
8. The special requirements must be clearly defined and laid down in writing.
9. The programmes must reflect the state of the art defined in scientific/economic/technical publications, standards or other generally recognised publications.

---

\(^\text{1078}\) EA, op. cit., 2014
Further requirements for programmes of certification bodies

In addition to the nine DAkkS requirements described before, a certification programme has to meet the requirements outlined in EA Document 1/22,\textsuperscript{1079} which was presented at the beginning of this chapter.

Use of DIN EN ISO/IEC 17067 is recommended for the development of programmes for product certification.

In addition, it is to analyse whether there are already existing accredited programmes with the same or a similar statement of conformity. If this is the case, the requirements must be comparable or the certification programme must be significantly different.

Additional requirements for CA programmes in the field of certification of PSS

For product certification, DAkkS refers to the ISO/CASCO toolbox, in particular ISO/IEC 17067, ISO/IEC 17065, ISO/IEC 17007 and ISO/IEC Guide 28, which was replaced by ISO/IEC TR 17026:2015. In addition to the standards of the toolbox for product certification, further requirements of product certification programmes are specified by the document IAF GD5. Selected requirements include:\textsuperscript{1080}

- The statement of conformity must refer to a clearly identified product, service or process.
- The requirements against which the products, services or processes are assessed must be clearly specified. The limits and tolerances must also be specified.
- If examinations or inspections are to be conducted during product certification, the method used must be proven to be appropriate for the relevant task. The procedure must also describe when and how samples are to be drawn.
- The programme must also describe the way in which the results should be evaluated and what consequences should follow from the results. This implies that deviations (non-compliance) which will lead to a rejection, suspension or revocation of certification have to be described.
- The programme must define requirements for personnel involved in the certification process.
- The programme has to give information on the (practical) details of surveillance (if applicable).
- The certification statement must agree with the investigation carried out.
- If certification is linked with the use of a CA certification mark, the requirements of ISO/IEC 17030 and ISO Guide 27 must be met.

By 2012, DAkkS had conducted 4,500 accreditations, including accreditations of laboratories, inspection and CBs.

\textsuperscript{1079} EA, op. cit., 2014.
\textsuperscript{1080} DAkkS, op. cit. 2014, p. 17f.
8.2.3. **ITALY**

L’Ente Italiano di Accreditamento (hereinafter ACCREDIA) is the Italian National accreditation body appointed by the state to perform accreditation activity according to the inter-ministerial decree of 22 December 2009, which was published in the Official Gazette, No. 20 of 26 January 2010.\(^{1081}\)

In terms of accreditation of security services and systems, Law Decree No. 115 of the Ministry of Interior, issued on 4 June 2014, regulates features and requirements for the certification of private security companies.\(^{1082}\) However, it is not accrediting CBs for security products at the moment. Only CBs for certification for ISO 27001 and ISO 20000\(^{1083}\) are accredited.

The ACCREDIA Executive Committee approved the accreditation under UNI/CEI/EN ISO/IEC 17065 Bodies. In July 2014, it approved new activities for professionals, products, services and management systems CBs. On the one hand, the following standards relating to security were issued:

- UNI 10891 certification\(^ {1084}\) for private security companies.
- UNI/CEI/EN 50518 – “Monitoring and Alarm Receiving Centres” for operative and remote monitoring centres.
- A series of measures taken to the railway rolling stock for fire protection from surfaces to light diffusers, from information devices for passengers on the floors and furniture, as well as electronic and mechanical equipment must be highlighted.\(^ {1085}\)

In addition, Circular No. 07/2015\(^ {1086}\) is an informative communication that describes the process of accreditation, recognition and maintenance of the following accreditation schemes: “Vigilance Organisations and their Services” (UNI 10891), “Monitoring and Alarm Receiving Centres” (UNI 11068/EN 50518) and “Security Professionals” (UNI 10459).

Regarding electronic documents and linked to the security field, Law Decree 7/2005 regulates the procedures for the accreditation and supervision of public and private bodies engaged in the preservation of electronic documents. In this regard, Article 44 of the above-mentioned

---

\(^{1081}\) “Designation of ACCREDIA as the sole Italian accreditation body to undertake accreditation and market surveillance activity in accordance with Regulation (EC) No. 765/2008, as per Article 4 §4 of the law of 23 July 2009, No. 99”; more information available at [http://www.accredia.it/](http://www.accredia.it/).

\(^{1082}\) Further information available at: ACCREDIA, Home, no date. [http://www.accredia.it/](http://www.accredia.it/).

\(^{1083}\) On the one hand, ISO 27001 is a best-practice framework for an information security management system that helps to identify the risks pertaining to important information and put in place the appropriate controls to help reduce them. On the other hand, ISO 20000 describes the requirements for an information technology service management system. All the information regarding the certificates are available on the ACCREDIA website: [http://www.accredia.it/psearch/accredia_companymask_remote.jsp?ID_LINK=266&area=7](http://www.accredia.it/psearch/accredia_companymask_remote.jsp?ID_LINK=266&area=7).

\(^{1084}\) UNI 10891 is an Italian certification which provides different types of services, such as security, watch robbery and shoplifting services, remote monitoring services, emergency response, safekeeping, transport and processing service for valuables and equivalent assets.

\(^{1085}\) This is a voluntary certification that excludes what is legally evaluated by independent verifiers for security and by notified bodies for high-speed rail and conventional rail (NoBo) interoperability; all this information is available at [http://www.accredia.it/news_detail.jsp?ID_NEWS=1625&areaNews=95&GTemplate=default.jsp](http://www.accredia.it/news_detail.jsp?ID_NEWS=1625&areaNews=95&GTemplate=default.jsp).

Decree and the Digital Administration Code (CAD)\textsuperscript{1087} state that the “Agency for Italy Digital is responsible for accrediting the public and private entities engaged in the preservation of electronic documents”.\textsuperscript{1088}

Ultimately, and due to the importance of security in Italy, ACCREDIA organised the meeting “Security & sustainability: The current role of certification”, which took place on 28 and 29 October 2010.

\subsection*{8.2.4. \textit{Slovenia}}

\textbf{Slovenian Accreditation}

Slovenian Accreditation\textsuperscript{1089} (SA) is the national accreditation body responsible for the establishment, development and maintenance of a professional, independent and impartial accreditation system in Slovenia. As a public institute established by the Republic of Slovenia, it performs accreditation as the only, independent and non-profit institution and represents the interests of the Republic of Slovenia in international accreditation cooperation. Its status as a public institute provides SA with the necessary independence and impartiality. In its contractual relationships, SA tries to avoid involvement with any natural or legal persons that could compromise the fulfilment of the principles of independence and impartiality in its work.\textsuperscript{1090} SA is managed by a director. The SA Board is the governing body and is composed of representatives of all interested parties within Slovenia, such as CABs, industry, trade, consumers, experts in metrology, and the state and professional associations. The technical work of SA is steered by the Accreditation Committee.\textsuperscript{1091}

SA has established and maintains an accreditation system for the following types of CABs: calibration laboratories, testing laboratories, inspection bodies, CBs for products/processes/services, CBs for management systems, CBs for persons, GHG emissions reports verifiers, and Environmental Management Systems (EMAS) verifiers. It also takes part in assessing the competencies of organisations wishing to be designated as Notified Bodies. The technical fields in which SA performs accreditation for particular types of CABs are diverse and comprise all the key activities encountered both in everyday life and in very specific environments, including security products, processes and services.\textsuperscript{1092}

\footnotesize
\textsuperscript{1087} The Digital Administration Code (CAD) is available at http://www.funzionepubblica.gov.it/media/615597/testo%20coordinato_decreto%20legislativo%2082%20del%202005%20coordinato%20con%20le%20modifiche%20introdotte%20dal%20l%20gs%20235%20del%202010.pdf.

\textsuperscript{1088} Literally, it is states the following: L’art. 44-bis attribuisce all’ Agenzia per l’Italia Digitale (di seguito “Agenzia”) il compito di accreditare “i soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi anche per conto di terzi e intendono conseguire il riconoscimento dei requisiti del livello più elevato, in termini di qualità e sicurezza”.

Agenzia per l’Italia Digitale, Presidenza del Consiglio dei Ministri, Modalità per l’accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi anche per conto di terzi e intendono conseguire il riconoscimento dei requisiti del livello più elevato, in termini di qualità e sicurezza”, Circolare n. 65, 10 April 2014.

\textsuperscript{1089} Slovenian Accreditation, no date. http://www.slo-akreditacija.si/


Legal bases

SA performs its tasks as the national accreditation service in compliance with the Accreditation Act\textsuperscript{1093} and the Decision on the Establishment of the Public Institute Slovenian Accreditation.\textsuperscript{1094} Its operation is detailed in the Statutes of the Public Institute Slovenian Accreditation.\textsuperscript{1095} Through the Technical Requirements for Products and Conformity Assessment Act,\textsuperscript{1096} SA is actively involved in the procedure of assessing the competence of CABs to work in the regulated sector (in cooperation with the ministry responsible for the market). SA operates in accordance with the regulation on accreditation and market surveillance,\textsuperscript{1097} which lays down uniform basic rules for the performance of accreditation, which represents the highest level of determining the competence of CABs.

The accreditation procedure at Slovenian Accreditation

SA operates pursuant to international standards and carries out its activities in a non-discriminatory way, implementing the principle of equal treatment of all CABs. When a CAB meets all the requirements of the accreditation standard, the procedure is concluded and an accreditation certificate, which confirms the client’s competence for carrying out the CA activities specified in an annex to the certificate, is granted. The accreditation procedure is carried out in three main steps, as described below.\textsuperscript{1098}

Pre-assessment

Pre-assessment is carried out in agreement with the client – it is not an obligatory part of the accreditation procedure. The purpose of pre-assessment is to find out whether the conditions for the performance of initial assessment have been fulfilled, and whether the scope of activity for accreditation has been stated appropriately.

Initial assessment

SA appoints an assessor team to carry out assessments based on the requirements of the relevant standard requiring competence on the part of the CAB; in so doing, they verify the fulfilment of technical and organisational requirements, professional competence, and the efficiency of the management system. At the conclusion of the assessment, the client receives an assessment report and, in the event of any nonconformity having been found, carries out the necessary corrective actions and reports them to SA. The assessor team then draws up a report on their examination of such corrective actions and makes a recommendation for a decision on accreditation.

\begin{thebibliography}{99}
\bibitem{1094} Government of the RS, Decision on the Establishment of Public Institute Slovenian Accreditation, Official Gazette of the RS, Nos. 36/00, 23/01, 121/04 and 22/08, http://www.pisrs.si/Pis.web/pregledPredpisa?id=SKLE997.
\bibitem{1095} Slovenian Accreditation, Statutes of the Public Institute Slovenian Accreditation, Official Gazette of the RS, Nos. 63/02 and 136/04, http://www.pisrs.si/Pis.web/pregledPredpisa?id=STAT70.
\bibitem{1096} National Assembly of the RS, Technical Requirements for Products and Conformity Assessment Act, Official Gazette of the RS, No. 17/11, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5804.
\bibitem{1098} Application procedure, no date, http://www.slo-akreditacija.si/accreditation_procedure#application_for_accreditation.
\end{thebibliography}
Decision on granting accreditation
After the assessment procedure has been successfully concluded, SA adopts a decision to
grant accreditation. SA issues an Accreditation Certificate to the body, including an Annex
specifying the scope of the accredited activities. Through the grant of accreditation, the organ-
isation obtains the right and duty to use the accreditation mark with own identification num-
ber, but only in relation to those activities for which it holds accreditation. Accreditation is
valid until withdrawn, i.e. as long as the organisation meets the requirements for accredita-
tion. Information on accredited bodies is publicly available on SA’s website.

Market surveillance
After the granting of accreditation, SA undertakes ordinary annual surveillance assessments to
check the fulfilment of the requirements for keeping it. Every four years a full re-assessment
is made. Accreditation is valid until withdrawn, i.e. as long as the organisation meets the re-
quirements for accreditation.

The number of accreditations per year
In 2013, SA issued five new accreditations (against 10 in 2012, 14 in 2011 and 15 in 2010,
which was still lower than the number in most other years in the recent past). On the other
hand, the number of accreditations held in 2013 was 228, against 237 in 2012 and 231 in
2011. The number of active accreditations has been generally increasing over the years.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of new ac-</td>
<td>40</td>
<td>40</td>
<td>34</td>
<td>16</td>
<td>12</td>
<td>17</td>
<td>19</td>
<td>15</td>
<td>14</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>creditations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of accredi-tions held</td>
<td>85</td>
<td>125</td>
<td>159</td>
<td>170</td>
<td>180</td>
<td>197</td>
<td>214</td>
<td>221</td>
<td>231</td>
<td>237</td>
<td>228</td>
</tr>
</tbody>
</table>

Source: Slovenska Akreditacija, 2013 annual report
Figure 142: Number of accreditations in previous years in Slovenia

Accreditation pertaining to security products and services
From previous research, it follows that there are four relevant security CBs in Slovenia:

- The Slovenian Institute of Quality and Metrology (SIQ);
- The Slovenian National Building and Civil Engineering Institute (ZAG);
- Bureau Veritas d.o.o.; and
- TÜV SÜD Sava d.o.o.

The Slovenian Institute of Quality and Metrology (SIQ) and the Slovenian National Building
and Civil Engineering Institute (ZAG) are the bodies accredited by the national accreditation
body, SA. The majority of certifications in the security field are based on the ISO/IEC 27001
standard (“Information Security Management”).
In the field of security certification (and also in other fields not covered by this research), SIQ is the most relevant Slovenian CB, with its own quality seal which is very well recognised and trusted. SIQ has affiliates in Croatia, Serbia, Italy and Germany. It also issues internationally recognised IECEE/CB test reports and certificates and internationally recognised EMC reports that enable global market acceptance of products.

As an independent institute carrying out testing and attestation of conformity of construction products, ZAG performs only two security-related certifications, based on standards EN 14339 and EN 14384.

SA is a full member of the EA, ILAC and the IAF. It takes an active part in the EA’s bodies, technical committees and task forces and in FALB, which enables it to have a direct influence on the direction and implementation of accreditation policy in Europe. Participation in the work of the EA is also one of the conditions for maintaining the signature of a Mutual Recognition Agreement. SA’s representatives actively participate in the following technical committees of the EA: the Inspection Committee, Certification Committee, Laboratory Committee, Horizontal Harmonization Committee, and Communications and Publications Committee.

**Advantages and disadvantages of the Slovenian accreditation framework**

The advantages of the Slovenian accreditation framework can be summarised as follows:

- Internationally recognised system;
- Harmonised approach to accreditation and internationally agreed standards;
- Independent public institute;
- Benefits for the quality of services and supporting international business; and
- Increases public trust in products and services.

Disadvantages include:

- The costs of accreditation (both internal and external);
- Potential differences between assessors; and
- Availability of resources for accreditation (see below).

SA is part of the public sector and as such has been subject to austerity measures which have impacted on the number of employees. The 2013 annual report draws attention to the lack of available resources, which might have an impact both on the efficiency and responsiveness of SA and on the fulfilment of international agreements. The current staffing level at SA is not

---

1100 International Laboratory Accreditation Cooperation, Home, no date, http://www.ilac.org/
always sufficient to cover a workload linked to the increasing volume of accreditation activities and the need to develop accreditation competence and projects in new fields.\textsuperscript{1103}

\subsection*{8.2.5. Spain}

The Entidad Nacional de Acreditacion (hereinafter ENAC) has been appointed as the Spanish national accreditation body according to Royal Decree 1715/2010. ENAC provides the Spanish market with an infrastructure of competent CABs that comprises 820 testing laboratories, 151 calibration laboratories, 228 inspection entities and 130 accredited CBs that operate in practically all economic sectors.\textsuperscript{1104} ENAC accreditation is recognised in over 70 countries. It is a signatory of all Multilateral Recognition Agreements (MLAs) established in international organisations of accreditation bodies: European cooperation for Accreditation (EA), International Laboratory Accreditation Cooperation (ILAC) and International Accreditation Forum (IAF).

In the field of security, ENAC accredits the following products and services:

- There are three alarm and private security elements certifiers. This field is practically regulatory so there is little scope for accreditation.
- Laboratories of Security PSS. There are five regarding to explosives, security software, the National Intelligence Centre (CNI),\textsuperscript{1105} safety boxes, bulletproof vest, gun smiths and data exchange protocol.

Some foreign organisations with a major influence on purchasing decisions (including industrial associations, non-governmental organisations and consumer organisations) have established schemes based on ENAC’s examples, which are therefore a \textit{de facto} requirement to access the relevant markets. In the field of industry, it can be outlined the accreditation between Engineers Ireland and the "\textit{Consejo General de la Ingeniería Técnica Industrial}" (COGITI).\textsuperscript{1106} They signed a memorandum of understanding and mutual recognition agreement.\textsuperscript{1107}

In the field of consumption (final consumers and users), two phases must be taken:

A. The application of accreditation. This is a process aimed at a candidate proposed by an association of consumers, companies or the Administration to formalise its commitment to the

\textsuperscript{1105} The Centro Nacional de Inteligencia is the public institution responsible for providing the Prime Minister and the Government of Spain with information, analysis, studies or proposals that enable the prevention and avoidance of any danger, threat or aggression against the independence or territorial integrity of Spain, its national interests and the stability of its institutions and the rule of law; see http://www.cni.es/en/welcometocni/.
\textsuperscript{1106} COGITI is the General Council of Spanish Technical Industrial Engineering. Official website is available at http://www.cogiti.es/Paginas/Ficha.aspx?IdMenu=A223BD0-3048-4D9D-AB8C-C91C6FDFD475&Idioma=es-ES
\textsuperscript{1107} Full document is available at http://www.coitigr.com/coitigr2013/tablon/PDFS/Convenio%20firmado%20COGITI-Engineers%20Ireland.pdf
arbitration system. All the obligations must be assumed by the candidate. If all the requirements are fulfilled, the candidate becomes an arbitrator in the Arbitration Board with their inclusion in the list of accredited referees.

B. If the application is removed from the list, the arbitrator accredited to the Consumer Arbitration Board loses its status.

Some changes have been made to the Spanish accreditation system as a consequence of the transposition of the Directive on Services in the Internal Market and Regulation (EC) No. 765/2008. More than 40 laws and regulations have been modified, including the Spanish Law of Industry and the Regulation of Infrastructure for Quality and Industrial Security. These legislative acts are aimed at eliminating barriers to competition. In this context, the following measures have been implemented:

A. A priori administrative control is replaced by a posteriori control (through communications or affidavits).

B. Public interest or public health are exceptions to this rule. Currently industrial security is not established as a public interest in Spain.

In view of recent developments in case-law, the main innovation has been the waiver on the obligation for prior administrative approval in the field of the security industry.

The Spanish legislator made an error in transposing the above-mentioned Directive by not considering industrial security as an overriding public interest. As a result, the quality of inspections, rigor and impartiality have been called into question.

The Spanish process of accreditation

ENAC has to comply with the requirements for certification specified in the ISO/IEC 17065 standard. In addition, the product, service or system must meet certain requirements (i.e., a series of evaluation processes).

In Spain, ENAC accredits entities according to their purpose, thus:

- ISO/IEC 17020: inspection bodies;
- ISO/IEC 17025: laboratories;
- ISO/IEC 17024: individual persons;
- ISO/IEC 21000 or 17021: management systems.

1110 It is established by the following case-law: the Supreme Court’s decision of 29 June 2011 (No. 2011/69), the Supreme Court’s decision of 21 February 2011 and, more recently, the High Court of Justice of Andalusia decision of 5 November 2012.
The SO sets the certification process beyond the standard EN 17065 (the minimum content of accreditation).

1. Scope of accreditation

ENAC establishes the requirements for an organisation to determine whether it has jurisdiction to act publicly/in the market. It monitors the certification scheme in all its phases. The application accreditation for a specific scope is a declaration on the part of the body of its technical competence for all the activities included in it, and the ENAC assessment, therefore, sets out to determine whether the body is capable of showing its competence in the whole of the scope declared. After receiving the application for accreditation, ENAC reviews the documentation supplied and checks if the activity is suitable for accreditation.

For laboratories, PAC-ENAC-LEC (5 July 2014) document sets out the specific process of accreditation. It informs the applicant of the dossier number assigned and the officer responsible for coordinating the accreditation process (checks the scope of the activities to be accredited is clearly defined and confirms that all the information needed for preparing and carrying out the assessment properly). If everything is correct and before starting the assessment, ENAC sends the applicant a cost estimate. In cases of non-compliance (i.e. documentation is incomplete or unsuitable), corrective measure must be taken by the applicant.

At an international level, ENAC may recognise accredited services in other countries. This international recognition occurs through various mechanisms, although they are all based on a common characteristic: the prestige and expertise demonstrated by ENAC at international level in different areas:

- Multilateral recognition agreements. By signing the MLA, accreditation bodies assure the equivalence of their accreditation systems and, therefore, that of the activities of accredited organisations, building cross-border trust and acceptance of information provided by accredited assessment bodies, regardless of the country in which they are located.

- Recognition by authorities. It is based on the provision of the Article 11 of Regulation (EC) No 765/2008.

- Recognition in the private field. ENAC accreditation is required by organisations in different countries that have established industry-wide assessment schemes, providing major international recognition to Spanish companies and products which have the backing of accredited certificates or reports. These schemes are generally established by conglomerate buyers or buyers associations that define special requirements for their supplies and demand that suppliers show compliance by way of the participation of an accredited conformity assessment body.

---

1112 The document is available at: https://www.enac.es/documents/7020/5054bb49-cf0d-4346-b191-61f6c8521ec
1113 ENAC, Accreditation Process, no date. https://www.enac.es/web/english/accreditation-process#paso01
1115 Art. 11 states that "National authorities shall recognise the equivalence of the services delivered by those accreditation bodies [...] and thereby accept [...] the accreditation certificates of those bodies and attestations issued by the conformity assessment bodies accredited by them."
2. Assessment

- Designation of the audit team. ENAC designates an audit team amongst its assessors and experts to carry out the assessment process.
- Documentation study. Prior to the on-site audit, a study is made of the technical documents supplied by the body. The report with the result of the study is forwarded to the body so that it may adopt the measures it considers fit for resolving, where appropriate, the problems detected.
- Auditing and accompanying visits. When the documentation analysis is considered acceptable, the assessor informs the body to set the date of the audit and forward an Audit Schedule in which the management system of the body, its operation, the undertaking of the activities and the accreditation requirements are assessed. Finally, the experts provide with a summary of the results of the investigation regarding to the accreditation criteria.
- Audit team report. Once the audit is fully completed, the body is given a written report with the results of the assessment carried out.
- Applicant’s response. The body should study the causes of nonconformities detected, review the impact and forward ENAC a schedule of corrective action.

3. Accreditation Decision

Formal accreditation is the final step. The Accreditation Commission is an independent technical body that approve formal accreditation. It tests the information generated during the assessment process and, on the basis of this, it may confer accreditation issuing an Accreditation Certificate.

During the term of the certificate, ENAC checks that accredited bodies continue to comply to accreditation requirements with regular assessments. If it is observed at any time that the body does not fulfill an accreditation obligation, ENAC may suspend or withdraw the accreditation temporarily until compliance with the accreditation requirement is demonstrated once more. In this regard, it ensures the process through a full verification suspending accreditation if the conditions do not conform to the standard ISO/UNE 17065:

- Stakeholders (producers, competitors, end-users, etc.) shall complete a questionnaire. The request shall be submitted in writing.
  The complaints will be assessed by the accredited entity although if they are repeated, ENAC might investigate and take disciplinary actions against the accredited entity involved.
- The certification authority shall file all claims if are required by ENAC; and
- Subsequently, ENAC shall decide whether or not suspend the accreditation.

---

1117 ENAC, op. cit., no date.
1118 ENAC, op. cit., no date.
8.2.6. Poland

The Polish Centre for Accreditation (PCA) is the national accreditation body authorised to accredit conformity assessment bodies on the basis of the Act of Parliament of 30 August 2002 on the CA system (consolidated text, Journal of Laws of 2014, Item 1645).

The general rules and policies applied by the PCA when conducting assessments or performing surveillance activities are presented in the document DA-01, which provides a description of the accreditation system, and in the other related documents. The PCA operates in accordance with requirements specified in the PN-EN ISO/IEC 17011:2006 standard “Conformity assessment – General requirements for accreditation bodies accrediting CBs”.

PCA currently conducts accreditation and surveillance processes over:

- Testing laboratories (DAB-07)\textsuperscript{1119}
- Calibration laboratories (DAP-04)\textsuperscript{1120}
- Medical laboratories (DAM-01)\textsuperscript{1121}
- Inspection bodies (DAK-07)\textsuperscript{1122}
- Product CBs (DACW-01)\textsuperscript{1123}
- Management systems CBs (DACS-01)\textsuperscript{1124}

\textsuperscript{1119} DAB-07 is a document which contains specific requirements. It includes general rules for granting and maintaining accreditation of laboratories and detailed rules for granting and maintaining accreditation of testing laboratories (accreditation requirements, accreditation in legally regulated areas, scope of accreditation, subcontracting for research, computational methods and calculation features of objects, study reports and a list of principles of evaluation laboratories research in the processes of accreditation and supervision). Further information available on: www.pca.gov.pl/doc/DAB-07.pdf

\textsuperscript{1120} DAP-04 document contains the following specific requirements: general rules for granting and maintaining accreditation of calibration laboratories and detailed rules for granting and maintaining accreditation of calibration laboratories (general requirements, scope of accreditation, requirements for lab personnel, proficiency tests, subcontracting in terms of calibration and evaluation of calibration laboratories in the processes of accreditation and supervision). In addition, additional information such as measurements, calibration certificate and certificate of measurement and calibration label is also included. Further information available on: www.pca.gov.pl/doc/DAP-04.pdf

\textsuperscript{1121} DAM-01 includes general rules for granting and maintaining accreditation of medical laboratories and detailed rules for granting and maintaining accreditation of medical laboratories (accreditation requirements, scope of accreditation a list of principles of evaluation of medical laboratories in the processes of accreditation and supervision). Further information available on: www.pca.gov.pl/doc/DAM-01.pdf

\textsuperscript{1122} DAK-07 includes general rules for granting and maintaining accreditation of inspection bodies and detailed rules for granting and maintaining accreditation of inspection bodies (accreditation requirements, scope of accreditation, and a list of principles of assessment of inspection bodies in the processes of accreditation and supervision including; technical measures and equipment, research capabilities, inspection reports and certificates of inspection, inspection training of staff, identification of locations where key activities are carried out, principles of inspectors and inspection election to observe the processes of accreditation and supervision). On the other hand, the process of accreditation and surveillance processes including supervision planned and reassessment, extending the scope of accreditation and detailed conditions for suspending or limiting the scope of accreditation are also included. Further information available on: www.pca.gov.pl/doc/DAK-07.pdf

\textsuperscript{1123} DACW-01 includes general rules for granting and maintaining accreditation of certification bodies, products and detailed rules for granting and maintaining accreditation, product certification (accreditation requirements, systems and certification programs, research capabilities, scope of accreditation and a list of principles of evaluation in the process of accreditation and supervision such as the process of accreditation, surveillance and reassessment planned, extending the scope of accreditation and detailed conditions for the suspension, withdrawal or reduction of accreditation). Further information available on: www.pca.gov.pl/doc/DACW-01.pdf

\textsuperscript{1124} DACS-01 includes general rules for granting and maintaining accreditation of certification bodies, management systems and detailed rules for granting and maintaining accreditation of management systems certification bodies, determining audit duration, scope of accreditation and a list of principles of assessment of management systems certification bodies in accreditation and surveillance processes (process of accreditation, surveillance and reassessment planned, expanding the scope of accreditation and detailed conditions for the suspension, withdrawal or reduction of accreditation). Further information available on: www.pca.gov.pl/doc/DACS-01.pdf
Regarding security accreditation, the PCA accredited the Institute of Security Technologies (MORATEX), a research institute supervised by the Minister of the Interior. This body conducts scientific studies and developmental work for the elaboration of new technological solutions in range of the individual protections as well as protection equipment.\textsuperscript{1129}

The laboratory is accredited by the PCA\textsuperscript{1130} within the scope of testing the physical, mechanical and usage properties of textile goods. The laboratory provides testing services to satisfy the needs relating to scientific and research activity for product certification and for customers.\textsuperscript{1131}

On the other hand, information security management systems\textsuperscript{1132} in Marshal offices in Poland must be highlighted. Lisiak-felicka and Szmit\textsuperscript{1133} analysed the implementation of information security management systems, evaluating their documentation, their information security administrator, and if there was adequate physical security of access to information and appropriate provision\textsuperscript{1134}.

\begin{itemize}
    \item Persons CBs (DACP-01)\textsuperscript{1125}
    \item EMAS verifiers (DAVE-01)\textsuperscript{1126}
    \item GHG verifiers (DAVG-01)\textsuperscript{1127}
    \item Proficiency testing organisers (DAPT-01).\textsuperscript{1128}
\end{itemize}

\textsuperscript{1125} DACP-01 includes accreditation requirements and conditions for granting and maintaining accreditation and certification of persons, detailed rules for granting and maintaining accreditation of personnel certification bodies. It contains a scope of accreditation and a list of principles of assessing personnel certification bodies in the processes of accreditation and supervision such as: the process of accreditation, surveillance and reassessment planned, expanding the scope of accreditation and detailed conditions for the suspension, withdrawal or reduction of accreditation. Further information available on: www.pca.gov.pl/doc/DACP-01.pdf

\textsuperscript{1126} DAVE-01 includes the accreditation requirements and specific program requirements (contract for certification, responsibility for decisions on certification requirements for resources, information available to the public, docs certification requirements for the process, application, review of the application, the first phase of the audit, the second stage of the audit, surveillance activities and, recertification). In addition, certificate and scope of accreditation, detailed principles of conducting the assessment of environmental verifiers in the processes of accreditation and supervision, the accreditation process (process of supervision, monitoring and reassessing planned, Limitation and widening the scope of accreditation and suspension and withdrawal of accreditation) and supervision on foreign verifiers is also included. Further information available on: https://www.pca.gov.pl/doc/DAVE-01.pdf

\textsuperscript{1127} DAVG-01 includes general rules on the accreditation, definitions and accreditation requirements (documents containing accreditation requirements, staff units), scope of accreditation, Detailed principles of assessment of GHG verifiers accreditation and surveillance processes (process of accreditation, surveillance processes composed by supervision planned and reassessment, limitation and extend the scope of accreditation and suspension and withdrawal of accreditation). Further information available on: www.pca.gov.pl/doc/DAVG-01.pdf

\textsuperscript{1128} DAPT-01 includes general rules for granting and maintaining accreditation of PT, detailed rules for granting and maintaining accreditation of the organisers of proficiency testing (accreditation requirements, scope of accreditation, Principles of assessing the organisers of proficiency testing in accreditation and surveillance processes composed by the process of accreditation, surveillance processes (planned supervision and reassessment, extension of the scope of accreditation and suspension of accreditation). Further information available on: www.pca.gov.pl/doc/DAPT-01.pdf


\textsuperscript{1130} It is accredited by Accreditation No. AB 154, Notification No. 1475, Directive 89/686/EEC – “Personal Protection Equipment”, and has accreditation from the Ministry of Defence.

\textsuperscript{1131} Specifically, flat textile products, products coated with rubber or plastics, rope goods, fibrous composites, plastics for personal protection goods making-up, technical making-up and personal protection means.

\textsuperscript{1132} The Information Security Management System (ISMS) is defined in the ISO/IEC 27000 standard as part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

ate security systems.

In this regard, in nine offices, of the 13 participating in the research, information security management systems were in place and key success factors were identified to implement the ISM, including employees’ awareness of the need to ensure the security of information, involvement of top management, definition of specific requirements for the system, substantive preparation workers and continue raising awareness for employees of all levels of the organisation and their respective substantive preparation.

The study from Lisiak-felicka and Szmit1134 continues examining the actions on the operation of the ISMS. In this regard, it reaches to the conclusion about the problems1135 officers encountered during the implementation of ISMS outlining some actions related to the improvement of the system and conducting the procedures for monitoring and maintenance of information security.1136

8.2.7. ROMANIA

The Romanian Accreditation Association (hereinafter RENAR) is a non-governmental and non-profit organisation, constituted according to Law 21/1924 with subsequent modifications. Its legal status was granted by decision number 1966/07.08.1990 (file 1975/PJ/1990) of the Civil Court of Sector 1, Bucharest.1137

RENAR is formally recognised as a unique national accreditation body by Government Ordinance 23/2009 and based on the provisions of Regulation No. 765/2008 and operates under the coordination and surveillance of the Ministry of the Economy. RENAR is thus authorised by the Government of Romania to accredit the following:

A. Certification Bodies

- The system of quality management (SMC) ISO 9001;
- The system of environment management (SMM) ISO 14001;
- Products and services;
- Personnel;
- The system of safety management (HACCP) ISO 22000;
- The system of health and occupational security management (OHSAS) 18001;
- The system of information security management (SSI) ISO 17799;

B. Testing and calibrating laboratories; and

C. Inspection bodies.

---

1135 The following problems must be noted: lack of use of formal methods of implementation of the system, insufficient financial resources, overly extensive documentation, lack of substantive preparation workers, and several problems of a legal and organisational nature.
1136 It says specifically, “Only a few offices can count on the support of government units in undertaking activities related to the implementation of the ISMS. It is worth noting the answer to the question on the frequency of ISMS review, which acted as a control question in the survey.”
In the field of security, RENAR does not accredit in the field of security products, but it has signed a collaboration convention with the Romanian Association for Security Technique (ARTS), which is an apolitical, non-governmental and non-profit legal person that promotes security in Romania. Ultimately, RENAR has signed a collaboration convention with The Romanian Association for Security Technique (ARTS), which is EURALARM member.

**8.2.8. The United Kingdom**

**The United Kingdom Accreditation Service**

The United Kingdom Accreditation Service (UKAS) is the sole national accreditation body recognised by government to assess, against internationally agreed standards, organisations that provide:

- certification;
- testing;
- inspection; and
- calibration services.

UKAS is a non-profit-distributing private company, limited by guarantee. UKAS is independent of the Government, but is appointed as the national accreditation body. UKAS’ involvement in international groups provides for mutual recognition, which reduces the need for multiple assessments of suppliers and as a consequence helps to reduce barriers to trade.

Since UKAS is a company limited by guarantee, it has Members instead of shareholders. The Members represent those who have an interest in all aspects of accreditation – national and local government, business and industry, purchasers, users, and quality managers. The board is supported in the day-to-day running of these activities by an Executive drawn from senior UKAS staff. The company takes advice on policy matters from a Policy Advisory Forum and on technical matters from a series of Technical Committees.\(^\text{1138}\)

**Legal bases**

UKAS is established by Accreditation Regulations\(^\text{1139}\) and EU Regulation 765/2008 and operates under a Memorandum of Understanding\(^\text{1140}\) with the Government through the Secretary of State for Business, Innovation and Skills (BIS). UKAS is licensed by the BIS to use and confer the national accreditation symbols which symbolise Government recognition of the accreditation process. A list of Management System Certification standards and normative documents covered under UKAS accreditation is maintained separately.

---


Accreditation procedure at UKAS

Upon receipt of an application, an Assessment Manager is responsible for taking the applicant through the accreditation process and for maintaining and renewing the accreditation in the future. The Assessment Manager discusses with the applicant the need for a pre-assessment visit and the composition of the proposed assessment team. The first visit to an organisation is arranged within approximately three months.

Pre-assessment visit
UKAS normally recommends a pre-assessment visit by the Assessment Manager (and possibly a technical assessor) to address the scope of accreditation requested. The Assessment Manager provides the applicant with a report on the findings of the pre-assessment.

Initial assessment visit
This is conducted by a Lead Assessor, supported, as necessary, by technical assessors with the expertise to cover the scope of accreditation. Prior to the visit, the applicant receives a visit plan, which provides a proposed timetable for the work to be assessed. Any improvement actions identified to meet accreditation requirements are notified to the applicant in writing during or immediately following the assessment visit. The applicant then needs to address the identified shortcomings. Once the improvement actions have been implemented to the satisfaction of UKAS, the applicant is granted accreditation.

Maintenance of accreditation
The accreditation is confirmed on an annual basis by surveillance visits, with a full re-assessment every fourth year. The first surveillance visit takes place six months after the granting of the accreditation.

Number of accreditations per year

The UKAS 2012/2013 annual report shows that in that period 3,439 accreditations were held. In total, 2,835 customers were accredited. UKAS has had 149 new customers and 66 leads and enquiries for developing new accreditation schemes. As Frenz and Lambert (2013) report, the demand for accreditation has grown by 50 percent over the last five years, substantially in non-traditional areas, including health testing and treatment-related technical services such as pathology and diagnostic imaging.

Accreditation of security products and services

The majority of accredited bodies and of transactions are in areas of technical testing and calibration, with particular emphasis on health services, such as diagnostic imaging equipment. The accreditation system also covers business process standards, mostly in connection with ISO 9001 and related standards, including Environmental Management Systems standards, for organisation and management. Accreditation in this field is carried out against ISO 17021.

Quality Management Systems and related systems can also be certified by bodies not accredited by UKAS – there is a market place in certification and in accreditation, some bodies offering their services based on reputation or price competitiveness. Others are accredited by bodies other than UKAS.

A number of CBs providing security-related certifications are accredited by UKAS. The majority of certifications in the security field are based on the ISO/IEC 27001 standard (“Information Security Management”). Also relevant are certifications based on ISO/IEC 17065 (“General Requirements for Bodies Operating Product Certification Systems”).

International membership of UKAS

The government recognises UKAS as the UK body, which will, where appropriate, negotiate mutual recognition agreements with other national accreditation bodies. In carrying forward its international work, UKAS has an obligation to seek and consider advice from a full cross-section of interests, including any relevant advisory committee established by UKAS. It will consult Government on all international accreditation issues where there is a significant Government or wider public interest involvement, whether as a result of a request from Government or otherwise.

UKAS has agreements within Europe through the EA and internationally through ILAC and the IAF. It is UKAS policy to negotiate agreements with other national accreditation bodies through the international and regional accreditation networks.

Frenz and Lambert (2013) note that international competitors in the fast-growing economies of China and India are committing substantial resource into the development of their own standards, accreditation and certification infrastructures in anticipation of benefits to their own trade, and believe that a strong UK presence in the international bodies on accreditation helps ensure that these do not form new barriers to UK trade.

---

1143 A full list is available on the UKAS website: http://www.ukas.com/about-accreditation/accredited-bodies/certification-body-schedules.asp.
1144 A full list of certification bodies is available at http://www.ukas.com/about-accreditation/accredited-bodies/certification-body-schedules-ISMS.asp.
1145 A full list of accredited bodies is available at http://www.ukas.com/about-accreditation/accredited-bodies/certification-body-schedules-PROD.asp.
1147 Frenz and Lambert, op. cit., p. 15.
Advantages and disadvantages of the UK accreditation framework

The advantages of the UK accreditation framework can be summarised as follows:

- building confidence in the work and the findings of CABs;
- impartiality;
- technical competence;
- UKAS accreditation offers a single, transparent and repeatable approach that may reduce the need for legislation and for government’s own assessment personnel;
- The UKAS Group achieved strong profitability during the year ending 31 March 2013, while at the same time it continued to invest in new areas of accreditation; and
- International membership of UKAS. ¹¹⁴⁸

One disadvantage might be the fact that UKAS is not the only organisation accrediting CABs in the UK. Therefore it needs to market its services and compete on the market (also because its work is primarily funded by accreditation services it performs for clients).

8.2.9. Other countries

To give an impression of the accreditation landscape not only in the EU but also in EU membership candidates, the following sections look at the situation in three such countries: Turkey, Albania and Montenegro.

Turkey

Turkey has a long tradition of European involvement and integration, and the country applied for EU membership in 1987. Although negotiations in general stagnated,¹¹⁴⁹ several positive aspects in the context of accreditation can be mentioned.

According to the European Commission Staff 2014 Progress Report,¹¹⁵⁰ Turkey showed some progress in the implementation of its risk-based electronic import control system, TAREKS. This covers mainly the “New and Global Approach” area, whereas most products in the “Old Approach” area must be licensed and approved before importing. This field still lacks appropriate conditions for free movement of goods.

Besides that, the engagement in CA also improved. The Turkish Accreditation Agency is a full member of the EA¹¹⁵¹ and covers 32 notified national bodies. While the EC report does

not provide data on security CBs, Turkey’s quality infrastructure in general includes 954 accreditations in 2014, reflecting an increase of 18 percent compared with 2013.\footnote{European Commission, op. cit., 2015, p. 27.}

The legislation referring to market surveillance has also expanded. Above all, Turkey has amended its overall market surveillance regulation. An operational database of the Ministry of the Economy supports border controls and activities to reduce the trade of products, which are non-compliant to relevant regulation. Nevertheless, ‘(e)ffective implementation of market surveillance is yet to be achieved.’\footnote{European Commission, op. cit., 2014a, p. 27.} In summary, efforts for free movement of goods have been improved, but some barriers to trade still exist.

**Albania**


According to the European Commission Staff 2014 Progress Report,\footnote{European Commission, Commission Staff Working Document, Albania 2014 Progress Report accompanying the “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Enlargement Strategy and Main Challenges 2014–2015”, SWD(2014)304/F1, 2014b, p. 22.} Albania shows some progress in easing free movement in goods, particularly in adopting core standards in the domains of telecommunications and electrical engineering. Moreover, the signing of the EA multilateral agreement on testing areas could soon be completed. So far, Albania’s Directorate of Accreditation is only an Associate Member in the EA (and listed as a potential candidate)\footnote{European Cooperation for Accreditation, *EA Associate Members*, http://www.european-accreditation.org/ea-members#2, accessed 5 March 2015.} but Albania is working to further align itself with European obligations.

The Albanian Law on Accreditation has been amended, and the country started the implementation of the ISO/IEC 17020:2012 standard for inspection bodies via its General Directorate for Accreditation. These efforts were supported by online and offline public-awareness activities. Moreover, market constraints have been reduced by an intensified alignment with the “New and Global Approach” legislation. Preparatory work continued, especially the revision of existing technical regulations.

In contrast, there is still room for improvement in market surveillance. Only two orders have been adopted: directions on standard mandatory operating procedures on the one hand and methods of risk classifications and assessment of serious risk on the other. A market surveillance inspectorate still needs to be established.
Montenegro

Montenegro applied for EU membership in 2008, after declaring independence from the State Union of Serbia and Montenegro in 2006. At present, EU institutions and Montenegro are negotiating over accession, after the country complied with central membership criteria in 2012.\textsuperscript{1157}

Montenegro’s progress regarding free movement of goods is rather limited. According to the European Commission Staff 2014 Progress Report,\textsuperscript{1158} the country is above all missing necessary capacities in its infrastructure bodies to cope with the broad harmonisation requirements. This leads to further issues.

First of all, the number of 21 accredited CABs remains relatively low. Moreover, Montenegro’s accreditation strategy for the years 2014–2018 had not been adopted by the time of the Commission’s study.\textsuperscript{1159} However, some positive developments can be observed, and based on the opening of Montenegro’s EU accession negotiations, the Accreditation Body of Montenegro became a full member of the European Cooperation for Accreditation (EA).\textsuperscript{1160}

Improvements can also be seen in the field of market surveillance. Some relevant amendments to the law and rulebooks for inspection have been established. Thereby, a significant amount of dangerous and high-risk products on the market could be eliminated. Furthermore, the parliament has adopted the “New and Global Approach” legislation.

\textsuperscript{1159} European Commission, op cit., 2014c, p. 21.
8.3. **INTERNATIONAL FRAMEWORKS AND ACCEPTANCE OF EUROPEAN CONFORMITY ASSESSMENT**

8.3.1. **INTRODUCTION TO INTERNATIONAL FRAMEWORKS AND MUTUAL RECOGNITION**

At the beginning of this chapter, activities of the International Accreditation Forum (IAF) and the International Laboratory Accreditation Cooperation (ILAC) were mentioned. The IAF facilitates cooperation between accreditation bodies accrediting certification and inspection bodies and the ILAC between accreditation bodies accrediting laboratories and inspection bodies.

Both entities provide for multilateral *mutual recognition arrangements between accreditation body members*. The IAF manages a Multilateral Recognition Arrangement (MLA), while ILAC operates an MRA. Both arrangements aim to establish confidence concerning the equivalence of the operation of the signatories to the agreement and that the results of accredited CABs issued under accreditation of the signatories are equally reliable. These multilateral *mutual recognition arrangements/agreements of competence at the technical level* between accreditation bodies have the ultimate aim of allowing products and services accompanied by accredited conformity attestations to enter foreign markets without the need for re-testing or re-certification in the import country. The objective of such recognition arrangements/agreements between accreditation bodies is therefore to contribute to reinforcing the acceptance of CA certificates.

Their work is facilitated by regional cooperation between accreditation bodies (RCABs), as established in:

- Europe (the EA);
- America: the Inter America Accreditation Cooperation (IAAC);
- Asia Pacific: the Asia Pacific Laboratory Accreditation Cooperation (APLAC) and the Pacific Accreditation Cooperation (PAC);
- Africa: the Southern African Development Community Accreditation (SADCA).

The IAF and ILAC arrangements are structured to build on these existing regional MLAs/MRAs established around the world. Except for SADCA, which is currently developing its regional mutual recognition arrangement, the above-listed cooperation organisations have agreements/arrangements in place within their region which the IAF/ILAC arrangements build upon as follows:

- **The IAF accepts the mutual recognition arrangements established within the EA and PAC**: accreditation bodies that are members of the IAF and signatories to the EA Multilateral Agreement (EA MLA) or the PAC Multilateral Recognition Arrangement (PAC MLA) are automatically accepted into the IAF MLA.
- **ILAC accepts the mutual recognition arrangements and underlying evaluation procedures of the EA, APLAC and IAAC**. Furthermore, accreditation bodies which are not affiliated to any recognised regional cooperation entity may apply directly to ILAC and/or the IAF for evaluation and recognition.

Signatories of both IAF and ILAC MLAs must recognise certificates, reports and results issued by organisations accredited by other signatories. This provides businesses with assurance...
that overseas bodies operate to the same standards and removes technical barriers to trade by eliminating redundant CA. This scheme may be summed up as in the following figure.

![Figure 143: Mutual recognition of laboratory and inspection team accreditation under ILAC](image)

Source: BIPM

Specific relations between the EA, ILAC and the IAF

EU Regulation 785/2008 has somewhat changed the relationship between the EA and ILAC and the IAF. As it defines, all European national accreditation bodies fulfilling the requirements of the Regulation automatically become members of the EA. Third-country accreditation bodies, however, may not necessarily meet all the above-outlined EU requirements, as these do not apply outside the EEA. This opens the need for rules regarding the relationship between the EA and international cooperation between accreditation bodies taking place within ILAC and the IAF and within their respective global Mutual Recognition Arrangement and Multilateral Agreement to which the EA belongs as a region.

If the EA recognised the equivalence among accreditation bodies and the equal reliability of accredited CABs only by accreditation bodies meeting the same requirements, it would undermine the international multilateral mutual recognition arrangement/agreements and isolate itself. As this is in no way the intention of the Regulation, the EA recognises that attestations of conformity issued in accordance with the requirements of ISO/IEC 17011 under accreditation bodies that are signatories to the ILAC MRA and IAF MLA but not signatories to the EA MLA or bilateral agreements (BLAs) and not complying with all the requirements of the EU Regulation are considered to be equally reliable from a technical point of view to those issued within the EA MLA and BLAs. Such a statement was formally endorsed by the EA General Assembly on 19 November 2008.

---

1162 European Commission, op. cit., 2013a.
In the following sections, the worldwide acceptance of European CA will be examined in both international and regional accreditation co-operations.

### 8.3.2. **The International Laboratory Accreditation Cooperation (ILAC)**

The history of the International Laboratory Accreditation Cooperation (ILAC) is an interesting one. While laboratory accreditation was first practised in 1947 to support the export markets from Australia, it was an initiative of the Under-Secretary of State from the U.S. Department of Commerce and his counterpart in Denmark that launched the development of accreditation at the international level.\(^\text{1163}\) They decided to hold a meeting in Copenhagen in 1977 to discuss concerns over documentation supporting food products being exported from Denmark to the US. The two countries extended an informal invitation to other governments and international bodies to attend the first International Laboratory Accreditation Conference (ILAC).

To their surprise, some 20 countries sent trade representatives along with organisations including the present-day Commission of the European Union (EU), the International Standards Organization (ISO) and the International Union of Independent Laboratories (UILI).

Later, as regional organisations (RCABs) were progressively being formed (APLAC in 1991, the IAAC in 1996, and the EA’s predecessors the WECC in 1975, the WELAC in 1989, the EAC in 1991 and the EAL (the merged WECC and WELAC) in 1994, the last eventually merging with the EAC to become the EA in 1997\(^\text{1164}\)), ILAC was formalised as a global cooperation in 1996, with 44 accreditation bodies signing a Memorandum of Understanding (MoU). It thus became a formal cooperation with a charter to establish a network of mutual recognition agreements among accreditation bodies.\(^\text{1165}\)

Since then, ILAC has met in plenary session on 20 occasions (over the past 25 years). Accreditation of quality management systems (QMSs) started in the early 1990s with the launch of the ISO 9000 series.

ILAC’s principal roles include:

- Recognition of competent test and calibration labs worldwide through its MRA, strengthening/deepening the MRA, promoting the use of accredited labs and appropriately linking this activity to the facilitated inter-governmental trade activity;
- Development and appropriate harmonisation of laboratory accreditation practice;
- Promotion of laboratory accreditation as a trade facilitation tool, including providing a clear distinction between certification and accreditation to help reduce the confusion in the marketplace, and increased cooperation with all relevant stakeholders, i.e. labs, regulators, industry groups, standard-writing bodies and governments; and

---

\(^{1163}\) Stanger, D. RING-II SD Project: Standards For Sustainable Trade, 4.11.2002

\(^{1164}\) DKD, “Mutual Confidence in Accreditation through Interlaboratory Comparisons – The Experience of EA”, no date.

• Providing socio-economic benefits at the national level and assisting in the development of laboratory accreditation systems by providing assistance to developing countries with pre-MRA support to their up-and-coming accreditation systems.

The ILAC Arrangement is the culmination of many years of intensive work. In November of 2000, an MRA was signed by those members who had successfully completed a peer evaluation. The list has been steadily growing since then. As of now (spring 2015), there are 89 signatories (Full Members) to the MRA, representing 74 economies, including almost all European economies. Furthermore, 16 Associate Members are seeking full membership status (including Albania, Belarus, Kosovo and Montenegro in Europe). 2009 data shows there being approximately 33,000 laboratories and over 6,000 inspection bodies accredited by the Full Member accreditation bodies.

Acceptance of an accreditation body into the ILAC MRA is dependent on its being successfully evaluated by peers from other accreditation bodies in accordance with the relevant rules and procedures contained in ILAC publications. Each accreditation body that is a signatory to the ILAC MRA commits to:

• Maintaining conformity with the current version of ISO/IEC 17011 and supplementary requirements documents and
• Ensuring that all laboratories that are accredited comply with appropriate laboratory standards (currently ISO/IEC 17025 – “General Requirements for the Competence of Testing and Calibration Laboratories” and ISO 15189 – “Medical Laboratories – Particular Requirements for Quality and Competence”).

The ISO/IEC 17025 standard lists the general requirements for the competence of testing and calibration laboratories and is the main ISO standard used by such laboratories. In most larger countries, ISO/IEC 17025 is the standard for which most labs must hold accreditation in order to be deemed technically competent. In many cases, suppliers and regulatory authorities will not accept test or calibration results from a lab that is not so accredited. Originally known as ISO/IEC Guide 25, ISO/IEC 17025 was initially issued by ISO in 1999. Since its initial release, a second release was made in 2005 after it was agreed that it needed to have its quality system words more closely aligned with the 2000 version of ISO 9001.

ISO/IEC 17020:2012 specifies requirements for the competence of bodies performing inspection and for the impartiality and consistency of their inspection activities.

27 of the 28 EU member states (all aside from Estonia) currently have a national authority that is a signatory to the ILAC MRA arrangement. Of the 27, all but four (Bosnia and Herzegovina, Ukraine, Slovenia and the Republic of Macedonia) have an authority that accredits in accordance with all above standards. These four are expected to add accreditation for ISO 15189 (Medical laboratories - Particular requirements for quality and competence) in the near future.

1166 The list of Full Members available at http://ilac.org/signatory-search/?q=all&id1xx=0&id2xx=0&id3xx=0&id4xx=0&pagenum=18.
1167 The list of Associate Members is available at http://ilac.org/ilac-membership/members-by-category/.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SERBIA</td>
<td>Accreditation Body of Serbia</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>AUSTRIA</td>
<td>Akkreditierung Austria</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>BELGIUM</td>
<td>Belgian Accreditation Structure</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>FRANCE</td>
<td>Comite Francais d’Accreditation</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>CROATIA</td>
<td>Croatian Accreditation Agency</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>CYPRUS</td>
<td>Cyprus Organisation for the Promotion of Quality (CYS) – Cyprus Accreditation Body (CYSAB)</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>CZECH REPUBLIC</td>
<td>Czech Accreditation Institute</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>DENMARK</td>
<td>Danish Accreditation</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>GERMANY</td>
<td>Deutsche Akkreditierungsstelle GmbH</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>NETHERLANDS</td>
<td>Dutch Accreditation Council</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>SPAIN</td>
<td>Entidad Nacional de Acreditacion</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>FINLAND</td>
<td>Finnish Accreditation Service</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>GREECE</td>
<td>Hellenic Accreditation System S.A.</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>HUNGARY</td>
<td>Hungarian Accreditation Board</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>BOSNIA and HERZEGOVINA</td>
<td>Institute for Accreditation of Bosnia and Herzegovina</td>
<td>YES</td>
<td>NO</td>
<td></td>
<td>YES</td>
</tr>
<tr>
<td>PORTUGAL</td>
<td>Instituto Portugues de Acreditacao</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>IRELAND</td>
<td>Irish National Accreditation Board</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>ITALY</td>
<td>L’Ente Italiano di Accreditamento</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
</tbody>
</table>
This concise coverage means that most, if not all, EU companies that have testing and/or calibration done in a laboratory accredited by one of these institutions should have significantly less trouble proving that a product conforms to the standards in countries that recognise ILAC-approved accreditations. As both the Asia Pacific region (APLAC) and the Americas (IAAC) have mutual recognition arrangements with ILAC, EU-tested products can enjoy a much higher level of acceptance in those economies.

As already stated, to achieve such a level of coverage, the ILAC MRA has been structured to build on existing and developing regional MRAs established around the world. Regional Cooperation Bodies which are operating a regional MRA coordinate peer evaluations and thereby maintain confidence in accreditation bodies that are signatories to the regional MRA. In turn, each Regional Cooperation Body that has been recognised by ILAC must also abide by the latter’s procedures and requirements and undergo routine peer evaluations by members of another Regional Cooperation Body or ILAC itself.

Source: ILAC1168
Figure 144: EU ILAC members and the standards they currently accredit to

Currently, the EA, APLAC and the IAAC are the only ILAC-recognised organisations. This means that the MRAs and evaluation procedures of the EA, APLAC and the IAAC have been peer-evaluated by ILAC and deemed to be satisfactory. Recognised Regional Cooperations are re-evaluated on an ongoing basis, over a four-year period, i.e. all aspects of the Regional Cooperation Body’s operation must be evaluated at least once every four years.

The end result of this network of mutual recognition is that test reports and calibration certificates issued by facilities accredited by a signatory to the ILAC MRA, will be accepted by the other signatories to the ILAC MRA and in some cases (the number is increasing all the time) by government regulators and industry.

8.3.3. The Inter-American Accreditation Cooperation (IAAC)

The IAAC is a regional association of accreditation bodies and other organisations interested in CA in the Americas. Its mission is to promote cooperation among the accreditation bodies and interested parties of the Americas, aiming at the development of CA structures to achieve the improvement of products, processes and services.

The IAAC plays a key role in the accreditation and CA by:

- Recognising the competence of accreditation bodies in the Americas;
- Creating a forum in which exchange of relevant information and consensus among accreditation bodies may be reached on important matters;
- Fostering multilateral recognition arrangements among accreditation bodies;
- Facilitating cooperation among member bodies; and
- Increasing knowledge and skills of staff to build and operate a reliable and efficient CA system in the Americas.

In Europe, the IAAC works in close cooperation with the European cooperation for Accreditation (EA).

8.3.4. The Southern African Development Community Cooperation in Accreditation (SADCA)

SADCA is a union of accreditation bodies in the Southern African Development Community (SADC) region; its aim is fostering cooperation and developing and maintaining mutual confidence. It is defined as a Technical Barriers to Trade Cooperation Structure established under the TBT Annex to the SADC Protocol on Trade.

1169 The Memorandum of Understanding (MoU) between IAAC and the EA is available on:

1170 “Technical Barriers to Trade” (TBT) Annex to the SADC Protocol on Trade Approved by the SADC Committee of Ministers of Trade on 17 July 2014, Gaborone, Botswana,
The African Cooperation in Accreditation (AFRAC) is one of the four pillars of the pan-African quality infrastructure established by the NEPAD Planning and Coordinating Agency to support intra-African trade, improve the competitiveness of African goods and services, and facilitate public health and safety and environmental protection.

On 29 September 2010 AFRAC launched its first meeting, at which representatives from the UK, Sweden and Germany and from Physikalisch – Technische Bundesanstalt (PTB) (Germany), the International Laboratory Accreditation Cooperation (ILAC) and the European Accreditation (EA) and others participants from all over the world took part. This may be seen as the first step taken by African institutions interested in international cooperation among accreditation bodies.

8.3.5. **The Asia Pacific Laboratory Accreditation Cooperation (APLAC)**

The Asia Pacific Laboratory Accreditation Cooperation (APLAC, [https://www.aplac.org](https://www.aplac.org)) was initiated in 1992 as a forum for laboratory accreditation bodies in the Asia Pacific region. Its primary aim is to establish, develop and expand a mutual recognition arrangement among accreditation bodies in the region.

To that effect, the APLAC Memorandum of Understanding (MoU), formally establishing APLAC, was signed in April 1995 by representatives from 16 economies in the Asia Pacific region. Further economies have joined APLAC since then. There are currently 37 signatories (of the 42 full APLAC members) to the MRA from a total of 24 regional economies.

The inaugural signing of the APLAC Mutual Recognition Arrangement (MRA) took place in November 1997. The MRA was extended in November 2003 to include inspection, and in April 2007 to refer specifically to ISO 15189 (the international standard applied to medical laboratories) that had previously been included under the “testing” scope of the MRA. The inaugural signing of the extended APLAC MRA to include accreditation of reference material producers (RMPs) took place in December 2007. The inaugural signing of the extended APLAC MRA to include accreditation of proficiency testing providers (PTPs) took place in June 2014.

Every signatory to the APLAC MRA is an operational accreditation body in the Asia Pacific region that has been through a comprehensive peer evaluation process and has demonstrated to the APLAC MRA Council that it operates in compliance with ISO/IEC 17011 and that its accredited facilities comply with ISO/IEC 17025 (laboratories), ISO 15189 (medical laboratories), ISO/IEC 17020 (inspection bodies), ISO Guide 34 (reference material producers) or ISO/IEC 17043 (proficiency testing providers).

Obligations of the APLAC MRA signatories include:

---


1172  Full members having also signed the APLAC MRA currently include Australia, Bangladesh, Canada, the People’s Republic of China, Hong Kong China, India, Indonesia, Japan, the Republic of Korea, Malaysia, Mexico, Mongolia, New Zealand, Pakistan, Papua New Guinea, the Philippines, the Russian Federation, Singapore, Sri Lanka, Chinese Taipei, Thailand, USA and Vietnam.

1173  APLAC, About APLAC, 2015. [https://www.aplac.org/about.html](https://www.aplac.org/about.html)
• Recognition of the accreditation of a laboratory, inspection body, RMP or PTP by signatories as being equivalent to an accreditation by its own organisation;
• Acceptance of endorsed calibration, test or inspection reports, reference materials certificates or proficiency testing reports issued by laboratories, inspection bodies, reference material producers or proficiency testing providers accredited by other signatories on the same basis as it accepts endorsed calibration, test or inspection reports issued by its own accredited laboratories and/or inspection bodies; and
• Recommendation and promotion of acceptance by users in its economy of endorsed test, calibration, and inspection reports, reference material certificates, or proficiency testing reports issued by organisations accredited by other signatories.1174

8.3.6. THE PACIFIC ACCREDITATION COOPERATION (PAC)

The Pacific Accreditation Cooperation (PAC) is an association of accreditation bodies and other interested parties whose objective is to facilitate trade and commerce among economies in the Asia Pacific region.1175 It has over 30 Full Members, representing most economies in the region, along with Associate, Observer and Corresponding members.1176

According to its webpage, PAC’s objective is rather similar to that of APLAC: the creation of a global system that grants international recognition of certification or registration of management systems, products, services, personnel and other programmes of CA.

To achieve this, PAC operates within the framework of the IAF,1177 as mentioned earlier, and in cooperation with other regional groups of accreditation bodies around the world. The primary means by which the IAF facilitates this is by the establishment of MRAs/MLAs which provide for worldwide recognition of certificates of conformity issued by certification/registration bodies accredited by IAF members.

The IAF, in turn, relies heavily on the MLAs of the three regional accreditation groups, the EA, PAC and the IAAC, as it is these groups which perform the majority of the peer evaluation activity rather than the IAF itself. Regional accreditation groups are evaluated every four years by the IAF. Membership of the IAF MLA is recognised as being satisfied by membership of any of the EA MLA, the PAC MLA or the IAAC MLA, within the appropriate scope.

Also, similarly to ILAC, the IAF evaluated and accepted the process and outcomes of ISO/IEC 17021 and ISO/IEC Guide 65 and the sub-scopes of ISO 9001 and ISO 14001.

1176 Members list is available at: PAC, PAC Members, 2009. http://www.apec-pac.org/content/pac-members
8.4. SUMMARY AND CONCLUSION

This chapter described international accreditation standards from ISO and their implementation in European Member States. In addition, it presented the European Cooperation for Accreditation and illustrated European framework conditions for accreditation and mutual recognition. It also showed types of certification schemes, specified by international standards, as well as requirements on certification schemes and scheme owners. The information will provide important guidance for the development of CRISP’s own certification scheme.

The international acceptance of European accreditations depends on the network of regional accreditation organisations, which provide for mutual review and recognition through international forums such as the IAF and ILAC.

European laboratory accreditation organisations are joined within the European Cooperation for Accreditation (EA). Their work is then recognised in the Pacific region through the IAF, and in the Pacific and Americas regions through ILAC. The stage is set for even greater mutual recognition as ILAC and the IAF are set to merge, further simplifying this process.

The international recognition of the European certification landscape is also documented in an ISO good practice guide, which describes the European approach as follows:

“The European Union […] has established a standardised system of laws that apply to all Member States, and uses ‘EU Directives’ to provide a legal definition of requirements for regulated products. The intention of EU product directives is that products can be sold across the EU without having to undergo repeated assessment and approval procedures. In some cases, their level of technical requirements has been diluted from those that were previously in place in some Member States before the EU was created. Nevertheless, they are equivalent to ‘technical regulations’, and lay down ‘essential requirements’ that regulated products must conform to. Market surveillance is conducted by designated authorities working through suitably qualified ‘notified bodies’. Compliance with the national standards that adopt the EN standards provides, by definition, a ‘deemed to satisfy’ method of meeting the essential requirements in the directives, although compliance with the standards is not in itself mandatory. Suppliers remain free to address the directives directly in any method of their choosing, but this is not always particularly easy. […] Two areas of good practice that have been highly developed over the last few years, and that have changed the regulatory scene dramatically, warrant further mention. These are the effect of the EU’s ‘new approach’ on technical regulation and the emergence of the EU’s RAPEX system.”

---

1179 The Rapid Exchange of Information System (RAPEX) is a European rapid alert system that “facilitates the rapid exchange of information between Member States and the Commission on measures taken to prevent or restrict the marketing or use of products posing a serious risk to the health and safety of consumers with the exception of food, pharmaceutical and medical devices, which are covered by other mechanisms” (source: RAPEX website, http://ec.europa.eu/consumers/safety/rapex/alerts/main/index.cfm?event=main.listNotifications).
According to the source, good framework conditions for the development of EU Directives for security PSS and their successful use to support the market exist.

8.5. REFERENCES


ACCREDIA, Home, no date. http://www.accredia.it/


Communication of the WTO Committee on Technical Barriers to Trade, “The use of the ILAC MRA and IAF MLA by central government bodies: the experience of the United States”


http://www.enac.es/documents/7435/cbe3baca-29e6-429a-b482-d4ad155117e5

ENAC, Accreditation Process, no date.
https://www.enac.es/web/english/accreditation-process#paso01


European co-operation for Accreditation, EA, *A briefing for European Commission Officials*.
http://www.european-accreditation.org/brochure/a-briefing-for-european-commission-officials


European Cooperation for Accreditation, EA Associate Members, http://www.european-accreditation.org/ea-members#2

European Cooperation for Accreditation, EA Full Members, http://www.european-accreditation.org/ea-members#1


International Accreditation Forum, IAF, no date, http://www.iaf.nu/
International Laboratory Accreditation Cooperation, ILAC, no date. http://www.ilac.org/

International Laboratory Accreditation Cooperation, ILAC, The list of Full Members, http://ilac.org/signatory-search/?q=all&id1xx=0&id2xx=0&id3xx=0&id4xx=0&papenum=18.


Memorandum of Understanding (MoU) between IAAC and the EA. http://www.iaac.org.mx/Documents/Controlled/Publications/PU%2020%20IAAC%20-%20EA%20MOU/PU%2020%20IAAC%20EA%20MOU.pdf


Pacific Accreditation Cooperation, PAC, About PAC, no date.
http://www.apec-pac.org/content/about-pac

Pacific Accreditation Cooperation, PAC, Pac Members, no date. http://www.apec-pac.org/content/pac-members.


Slovenian Accreditation, no date, http://www.slo-akreditacija.si/

Slovenian Accreditation, About Slovenian accreditation, no date,


9. **SUMMARY**

9.1. **GENERAL ASPECTS**

CRISP’s overall aim is to assist in the harmonisation of the European security market by developing a pan-European certification scheme. Stakeholders from the security field, which have been consulted so far in the project, support the notion of a European certification scheme for security PSS. A pan-European certification scheme and robust European standards are needed.

Whilst the current fragmentation of the European security market might well be viewed as a troubling situation, this relative dearth of existing programmes and schemes certainly represents an opportunity for the CRISP project to identify and promote the virtues of multinational pan-European certification schemes for security and to provide useful solutions that can foster pan-European programmes.

CRISP workshop attendees suggested that European standards could be based on strong national standards, so as not to ‘reinvent the wheel’. In this respect one might assume that what constitutes a strong national standard is one that is still used despite International or European standards existing within the same field. To determine this would need a consistent research approach as there can be other reasons for lack of take-up of ISO or EN standards.

Whilst there is evidence to support pan-European procedures and schemes, this is not without problems. Bouchard et al., for example, highlighted that ‘promoting effective multilateralism requires active involvement and commitment on the part of the whole (European) governments, not just of the Ministries of Foreign Affairs and Defence’.\(^\text{1180}\) Following this, van Schaik and ter Haar conclude that as long as other Ministries are not directly involved, the promotion of effective multilateralism will not be fulfilled. Another obstacle, mentioned by an interviewee is the lack of willingness by CABs to agree on common quality measures and auditing approaches, multilateral supervision and round robin tests. In summary, it is essential to appropriately and convincingly demonstrate the importance and need for wider adoption of pan-European, multinational security standardisation and certification, with solutions that address the different sectors of the security market.

CRISP’s work package 2 and the current report provide helpful information for CRISP’s further activities. The findings on accreditation were used for task 3.1 requirements for a harmonized approach. The material on the certification of drones are used for work package 4 and its in-depth analyses of relevant certification schemes. Criteria of the U.S. Safety Act were used to enrich work package 4’s STEFi criteria. In addition, the results provide an important foundation for CRISP’s roadmap and its certification manual.

---

9.2. **SPECIFIC RESULTS**

In the following sections we will present specific national findings, which show the varying and complex framework conditions for security standards and certification in the Member States but also good practice.

Differences of the security certification landscape include, for example, the different country size and protection needs, the different size of the national markets for security solutions and of the security industries, different structures of this industry and its market segments as well as different needs regarding security certification.

Certification services are offered by private certification bodies, industry organisations and governmental bodies, by accredited organisation and others as well. Many multinational certification bodies are also active in the Member States. Their fundamental procedures are identical and links between the different subsidiaries exist. Nevertheless they have to offer different certificates based on the requirements of numerous national security standards.

Another observation was that Europe’s security industry includes many security service companies (e.g. in Austria). In the CRISP context, services for security systems are particularly important. The new standard EN 16763 Services for fire safety systems and security systems will provide a foundation to offer harmonized certification services for these companies.

The country studies also show good practice in many areas. More information is given in chapter 9.3.

The study also highlights additional need for action. There are Member States in which a significant number of the security certification bodies are not accredited. Nevertheless the certificates are, for example in the Netherlands, widely accepted and there does not seem to be a strong interest in accreditation. A similar situation exists in Austria. Accredited certification bodies are not very important in the security sector. The demand for such certifications is rather low.

Barriers regarding mutual recognition on a European level were also unveiled. An example offers the certification of safes based on the national standards SS 3492 and SS 3493 in Sweden besides certificates based on multinational standards.

Findings of the country studies in detail:

The Austrian country study highlighted potential problems of regulations developed by non-accredited national security associations. In several cases, alternative European and international standards are not available. Nevertheless the risk of developing own national standards, which are especially tailored to fit the members of specific industry associations, is regarded as an important issue.

An interesting example in the Belgian country study is the INCERT certification scheme for intrusion detection, which is used by several certification bodies and which is quite popular in the country. Belgium is not particularly active in producing homegrown security standards, mainly having standards dating back from the 1970s and 1980s. The industry uses NBN ENs or the NBN ISO standards. Apart from standards, there are other normative documents...
Good practice examples in the French case study include, for example, the cooperative arrangements of AFNOR and CNPP with other European certification bodies. The country study also highlighted a specific need for cross-border solutions and interfaces. Consistent with a suggestion of CRISP’s stakeholders, the country study illustrates potential benefits of analysing concepts and solutions of other Member States or even adapting solutions from other national players. The country study also shows specific certification schemes for security services which build on national standards. This will be an important issue regarding the implementation of the new EU standard for security services.

Germany provides an advanced security certification infrastructure. An indicator for the success of its certification bodies is the high number of foreign subsidiaries. In addition to Germany’s involvement in European and international standardisation, specific security-related documents were created on a national level for areas in which no European or international standards exist. A number of these standards have interesting features for potential use for certification on a European level. Besides national, European and international standards used for certification, important market players with specific proprietary guidelines exist. Besides security certification, many specific certificates for different data protection fields are available. There are several interesting collaborative approaches such as ARGE DIN 14675. Good practice does not only characterise the common, standard-based certification scheme but also the collaboration between certification bodies and their stakeholders as well as the ARGE’s procedures to update its certification scheme. Much can be learned from the ARGE regarding the implementation of new European certification schemes (for services and for products as well). Concerning other key CRISP topics, there are accredited programmes for the certification of video surveillance systems and alarm systems. In addition, numerous projects of the national security research programme have developed evaluation methodologies, which might offer potential for developing appropriate certification solutions in new research fields. Interestingly, several evaluation concepts also consider ethical aspects, which are of particular interest for CRISP.

Good practice was also identified in the accreditation field. The German DAkkS is able to accredit specific security certification programmes and schemes, which build on documents with restricted access. While the relevant certifications build on guidelines and specifications, which are only available for selected persons entrusted with security duties, the DAkkS ensures that protection of the relevant information is not touched by the accreditation process.

Poland has a small security industry and only a few domestic security certification bodies, which use European standards for certification but also national documents and other guidelines. In addition, there are several subsidiaries of foreign certification bodies. CRISP’s new solutions will give certified domestic security companies the opportunity to access new markets without extra effort.

Slovenia, as one of the smallest EU Member States has not set any national standards in the field of security. European and international security standards are used. This will facilitate the implementation of new European standards and certification schemes. The current certification services mainly refer to IT security. Since CRISP’s focus is on PSS, new business opportunities based on the new scheme might occur. Due to the smallness of Slovenia’s security
industry, more research is necessary regarding the implementation of such services in the national market or the use of alternative certification services abroad.

The **Spanish** security certification landscape is shaped by several interesting characteristics. AENOR for example is not only responsible for security standardisation but also for certification and it offers many standards-based certificates. Due to this specific combination of duties, AENOR could become an important partner for promoting European security certification solutions in the future. The country study also offered an interesting example of the international TEMPEST certification but there are also challenges. According to an interviewee, the characteristics of external and accredited, independent and impartial certification bodies, are interpreted in a flexible way. The relevant organisations do not guarantee the access to international markets because they are not controlled by an independent third party. This is an important issue which requires more research efforts. Stakeholders also express their burden of different inspection requirements. They regard it as ‘nonsense’ that different requirements exist for example in Madrid, Barcelona or Andalusia. Another interesting feature of Spain’s security certification was developed recently. Spain offers an advanced approach to certify civil drones.

**Sweden**’s success of the StairSec certification programme laid the foundation of AEO. Interesting future-oriented standards have been developed for European ABC systems and CBRN protection. In addition, Sweden has one of the few security classified CBRN laboratories in Europe. Nevertheless, challenges were also unveiled. In particular they are related to several current certification services, which build on national standards alone.

The country study of the **Netherlands** highlighted an important issue: only a small part of certification in the national security sector is executed under accreditation. Even though most security certification schemes are not accepted by the Accreditation Council, the certification are widely accepted and acknowledged. Especially for the security service providers, there is a wide range of certification systems to choose from. This implicates confusion. As an expert stated, there seems to be a need for closer cooperation between sector organisations ‘to get to preferably one clear quality system for the security sector’.

CRISP’s Deliverable 3.1 describes several concerns over national requirements in the case of pan-European standards and certification schemes. A good practice example could be considered to be the **British** Loss Prevention Standards (LPS) offered by BRE and the ways in which additional requirements are added on to existing standards for certification of security products. This mechanism is reported to work well and could be used to respond to additional requirements for specific cases within the CRISP scheme. The UK also offers good practice examples in two innovative areas: video analytics and biometrics. BRE’s Video Analytics Assessment Programme also gives an example for an outsourcing of security certification functions from the government to private certification bodies. Although the Video Analytics Programme is regarded as good practice, its focus is on technical issues only. Ethical aspects are not included.

Besides the ten European countries analysed in this report, interesting approaches also exist in additional EU countries. Lewis (2014), who was quoted several times in this document, mentions for example the **Irish** National Standards Authority which offers certification for CCTV and video technology as well as access control systems. More Information is given at http://nsai.ie/Your-Industry/Security.aspx. Its services include an interesting certification
scheme for CCTV systems and installers based on the EN 50132 series of standards and certification based on ISO 28000 Supply Chain Security (but also certification based on national standards).

Several country studies highlighted the important role of services in the security market besides products and systems. Consistent with Wurster et al.\textsuperscript{1181} this also shows the importance of also considering security services in CRISP’s future activities. In addition, the CoESS (2001)\textsuperscript{1182} report shows that different legal framework conditions for offering security services exist in the Member States. Even the licencing of private security guards is not mandatory in all Member States. Therefore, the development of common solutions requires more analyses and research activities.

The case study of the United States provides good practice in several fields, which are described in more detail in chapter 9.3. Regarding specific standards, FIPS (Federal Information Processing Standards) has been very successful in the past. In particular, FIPS 140, which deals with the processing of sensitive data, is important. The advanced approach of the NIST towards privacy engineering was another interesting aspect. SIA’s Code of Professional Ethics provides an example for the inclusion of ethical aspects in security-related certification. The country study also provides an example for the handling of different security seals and the use of common standards by UL and Intertek. In addition, an interviewee highlighted the importance of shrinking product development cycles and the need for faster certification processes and standards development. He also emphasized the importance of performance-based requirements and of use cases for standardisation and certification. In addition he described the need for interoperable solutions and paradigm shift from product-centric security devices and systems to integrated systems which define a new demand for specific standards.

The Canadian case study highlighted many advantages of the Canadian standardisation system. The main advantage is legal certainty. The standardisation is based on a very tightly-regulated process which results in greater legal certainty. In addition, each of the SDOs writes standards with a high added value due to their vast experience and high level of knowledge. There are only four SDOs carrying out the process of standardisation and certification. Therefore, the system is highly manageable. Furthermore, SDOs are highly skilled and experienced at creating a strong and consistent process nationally and internationally recognised. The system has the Common Criteria Evaluation and Certification Scheme (CCS) which is highly efficient thanks to the maple red leaf, a well-known certificate. However, the Canadian system is subject to opening international markets. Therefore, SCC faces with one of its biggest challenges because it must regulate the system in a more open way and at the same time, it is seen as a reliable approach to control the entire process of standardisation.

In relation to the FIFA world Cup 2014 and the 2016 Olympic Games, Brazil has faced specific security issues. Compared with Europe, an important difference is that many aspects of security-related CA are managed by the State and governmental organisations. The national standards body ABNT is only partly involved in security standardisation. The case study unveiled in particular three aspects to learn from. The most interesting aspect was, that

\textsuperscript{1181} Wurster, S. et al., op. cit., 2014 (included in the relevant chapter of this document)
\textsuperscript{1182} Confederation of European Security Services (CoESS), op. cit., 2011 (included in the relevant chapter of this document)
in contrast to most European countries, ANAC, the agency responsible for aviation security is accredited by the national CB. In addition, the country study unveiled interesting activities regarding the certification of drones. It also highlights that it is not only necessary to develop certification infrastructures but also to implement mechanisms which allow an appropriate upgrating by the countries involved.

The **Indian** case study found that since the 2008 Mumbai terrorist attacks security expenditure has been steadily increasing and as a result India’s homeland security spend is now larger than the defence budget of many countries. Analysis of the Indian security market reveals that it consists mostly of electronic products and that the majority of security equipment is imported from Germany, US, UK and Japan. With regard to standardisation, the overall policy of the Bureau of Indian Standards (BIS) is to harmonise national standards with international norms and ISO standards. There are however still a number of national standards still in use. As can be seen in the Indian case study the great majority of listed standards and standards still in draft are harmonised Indian standards. With regard to certification, there are a number of certification bodies which work within India, which include both national and international organisations. With regard to best practice examples, we wish to highlight the Common Criteria (IC3S) scheme for IT security products, which is a recent addition to the certification landscape in India. The scheme provides national certification, once assessment is through and also provides framework for international certification through the International Mutual Recognition Arrangement with the other member countries of Common Criteria Scheme.

The **Israel** country study highlighted that the country has implemented state of the art security solutions, especially regarding cyber security. Overall, security and developing security solutions has a high priority within the country. For this reason, Israeli security technologies are regarded as influential and innovative worldwide. As the only statutory standards institution, the SII is involved in several security-related ISO Technical Committees, as well as operating product and system certification programmes and granting products and systems with SII marks. It was pointed out as well, that there is a trend in Israel to adopt to multiple, proven international standards (such as the European CE mark). Although there have not been set yet national standards in the Israeli secure standardisation landscape, as Israel is represented in international standards organisations (such as ISO and IEC) Israeli approaches and expertise can be integrated or proposed within certification and standardisation boards.

In **Japan**, the Japanese Industrial Standards Committee (JISC) is the body that maintains new and existing Japanese industrial standards (JIS), and is responsible for ensuring their compatibility with respective international standards, though participation in relevant ISO/IEC committees. Approximately 40 percent of JIS standards are currently identical to respective ISO/IEC standards, 57 percent were altered to some degree, and 3 percent are substantially different. The international standardisation activities are facilitating Japan’s economic recovery and growth, and enhancing its competitiveness in global markets. Particularly important in this context is the technical cooperation between Japanese and EU authorities in the CENELEC, CEN and a bilateral EU-Japan CA working group. Interesting aspects regarding certification include Japan’s “Guide for the improvement of (management system) certification” and the “Japan Initiative for Reliability Enhancement of Certification (JIREC)”. Regarding specific security aspects, Japan’s current activities in nuclear security may specifically enrich international standardisation in this field.
In the chapter of **international certification schemes** we analysed international security assessment solutions, partly in form of standards, partly in form of legal regulations, frameworks, partnerships or initiatives, from different (supra-)national organisations and institutions. These security assessment solutions provide a good insight into harmonisation processes of security PSS apart from important standardisation organisations and help in CRISP to map the wide field of security standardisation and certification. The selection is based on best practice examples but also shows the challenges with which they are confronted.

The solutions range from standards for a common video interface in CCTV systems (ONVIF), over the international code of conduct for security services, the European Privacy Seal (EuroPriSe), Nuclear Security Standards of the IAEA, to different cargo and supply chain security standards like the WCO Framework of Standards to Secure and Facilitate Global Trade, Customs-Trade Partnership Against Terrorism (C-TPAT) or the Container Security Initiatives (CSI).

The study on the Common Criteria framework showed that Common Criteria “delivers proof of quality and the reliability of the (security) product and offers the basis for the comparison of results of independent evaluations”. Notwithstanding the shortcomings and challenges of the framework, the CC are considered a best practice. Among the main success factors are the engagement of the public and private sector, the solid basis on the ISO/IEC 15408 standard, the mutual recognition of certificates in participating countries worldwide, the protection profiles and evaluation levels and the updated procedures which facilitate the response to new risks.

The **Accreditation** chapter described international accreditation standards from ISO and their implementation in European Member States. In addition, it presented the European Cooperation for Accreditation and illustrated European framework conditions for accreditation and mutual recognition. It also showed types of certification schemes, specified by international standards, as well as requirements on certification schemes and scheme owners. The information will provide important guidance for the development of CRISP’s own certification scheme.

### 9.3. **Identification of Good Practice Approaches**

This report identified attractive technical solutions, interesting examples for collaborations among certification bodies as well as approaches to consider societal aspects in security-related certification. In addition to the pioneers in harmonisation and mutual recognition in different security areas previously described in chapter 6 of CRISP’s deliverable 2.1, this report could identify more good certification practices on national and multinational levels.

There are a few security certification schemes in specific technical areas in the Member States, which avoid the narrow regional focus on national standards. ECB’s consequent orientation on **European and international standards** and its collaboration with various laboratories in different Member States is an interesting example in this regard.

---

1183 Aizuddin, Ariffuddin, op. cit., 2001
A good practice example regarding **collaboration** is the ARGE DIN 14675, established by the German TÜV Rheinland. ARGE DIN 14675 is an association of currently ten accredited certification bodies and the owner of an accredited certification scheme for the planning, operating and maintenance of fire alarm systems and voice alarm systems based on the DIN standard on ‘Fire detection and fire alarm systems - Design and operation’. Good practice does not only characterise the common, standard based certification scheme but also the collaboration between certification bodies and their stakeholders and the procedures to update the relevant certification scheme.

An important example to learn from on an international level is provided by the **U.S. SAFETY Act**, which applies to a wide range of security solutions. Another good practice example from the U.S. is the National Strategy for CBRNE Standards to overcome the coordination problem caused by the high number of agencies responsible for CBRNE standards.

Societal aspects of security systems are another important aspect to consider, in particular regarding surveillance solutions, because "(u)nseen, uncontrolled or excessive surveillance activities (...) pose risks that go much further than just affecting privacy. They can foster a climate of suspicion and undermine trust"\(^\text{1184}\)

Examples for partial response to this statement already exist in the certification field. Besides **EuroPrise**, a certificate for IT products, the British **CCTV Code of Practice** for CCTV systems example considers several specific aspects of freedom infringements. More information has to be collected on how this is translated into standardised requirements for the relevant certification schemes. The VdS 2365 on CCTV systems also integrated a few issues of that kind in its certification process but does not consider the full variety of CCTV-related freedom infringement aspects. More detailed examples for the partial inclusion of privacy aspects and freedom infringement in national certification schemes are given by CRISP’s deliverable 4.3. A Pan-European approach, which considers the whole variety of freedom infringement aspects of physical products and integrated digital-physical systems does not exist. A common solution for the integration of this social dimension is needed.

### References


#### 9.4. **RECOMMENDATIONS FOR CRISP’S FURTHER WORK**

Based on the analyses of the country studies, the multinational standards and certification schemes, nine recommendations are derived for the further work on the CRISP scheme, its implementation and usage.

---

Fast certification processes

As this CRISP report as well as the previous CRISP deliverables have shown, the security market is growing and demanding new secure, efficient, trustworthy PSS, which also take into consideration the freedom and rights of citizens. In this regard, faster certification processes and a shorter developmental period for standards are needed. There is also a need for certification organisations and institutions for better solutions in order to continuously improve and accelerate their proposed services on certification for security PSS.

Embeddedness in the socio-technical context

To avoid redundancy, the design of the CRISP scheme should take into account the structure and content of well-established national and international standards, where additional requirements can be developed on top of existing ones. The standards currently under development (for example at the international level) should also be carefully examined to the extent that the development is of a public nature, in order to search for similarities and synergies in approaches.

Its needs to be taken into account that the extent to which the CRISP scheme will seek compliance with national legal requirements, will most likely affect the adoption of the scheme. If certification will not seek a high enough level of compliance with national legislation, regarding freedom infringements for example, this might result in lack of interest in such certification.

Performance-based requirements

Furthermore, a trend towards performance-based requirements in certification has been identified. CRISP shall therefore consider the function of security PSS within its further research activities, as well as the need for performance standards. In this regard, an active exchange by concrete use cases between practical experts and researchers is highly recommended. This will work to assure that project findings will meet essential requirements and serve to keeping standards and the development of certification processes up-to-date.

Interoperable solutions

In the course of this deliverable, the importance of interoperable solutions was highlighted to enable security integrators to develop systems, whose components from different vendors can communicate with each other. Within CRISP’s further research activity, this has to be taken into account.

Implementation of the scheme

The diverse landscape of existing standards related to security PSS, coupled with a network of CABs that may or may not be accredited, requires careful consideration of how the certification scheme developed by CRISP will fit in into these existing relationships between CABs, accreditation bodies and end-users. Which CABs may be appropriate to certify under the developed scheme and whether accreditation of CABs will be relied upon are only some of the questions that the CRISP project will continue to seek answers to.
Accreditation practice

An important issue to reach transparency and fair competitiveness among security certification entities is the harmonisation of guidelines for their accrediting auditors. Cross trainings of accreditation auditors, mutual assistance between them and the reduction of differences among accreditation programs are needed in order to avoid substantial different test results in the same certification scheme.

As added value of certification is well recognised by stakeholders, it would be appropriate to invest efforts in the requirement of certification (not voluntary but mandatory) by accredited entities. The role of the government (public administration) is very important in this area (introducing standards in legislation and supporting the accreditation as a tool for the implementation of its policies).

Regular follow-up controls of certified solutions

As CRISP’s analyses showed, regular follow-up controls of the certified security PSS are significant. The certificate should represent the actual compliance or quality of the product or service. With regular compliance control, the certified entities have an additional incentive to keep improving or at least maintain an adequate level of compliance or/and quality. This also promotes trust in the certificate and the relevant security solutions.

Solutions for SMEs

The costs of certification must not be a competitive barrier for small and medium enterprises. First ideas include the adjustment of costs to the size and complexity of the entity as well as measures to ensure equal treatment of customers independent of their geographic location and the residence of the auditors.

Political support

The adoption of a new pan-European approach to certification for security PSS will necessarily require political support, as it follows from CRISP’s research in WP 2 and WP 4 that standards are heavily intertwined with national legislations. Further work on the development of strategies for the adoption of the CRISP scheme must therefore also focus on the political dimension of the European security certification landscape to receive appropriate support.