Report on the scenario-based workshops and the refinement of the CRISP Methodology

Hempel, Leon; Hirrschman, Nathalie; Haponava, Tatsiana; Von Laufenberg, Roger; Wurster, Simone; Wadhwa, Kush; Sveinsdottir, Thordis; De Hert, Paul; Kamara, Irene; Pauner, Cristina; Viguri, Jorge; Garcia, Rosario; Burnik, Jelena

Publication date: 2016

Document Version: Accepted author manuscript

Link to publication

Citation for published version (APA):
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 D5.2:
Report on the scenario-based workshops and the refinement of the CRISP Methodology

Authors & Contributors: Leon Hempel & Nathalie Hirschmann (TUB-CTS) & Tatsiana Haponava (NEN)
Roger von Laufenberg (VICESSE); Simone Wurster (TUB-INNO); Kush Wadhwa & Thordis Sveinsdottir (TRI); Paul de Hert & Irene Kamara (VUB); Cristina Pauner, Jorge Viguri & Rosario García (UJI), Jelena Burnik (IP-RS)

Dissemination level: Public
Deliverable type: Final
Version: 1
Submission date: 1 February 2016
Table of Contents

List of selected abbreviations..................................................................................................... 4
List of Figures ............................................................................................................................ 5
List of Tables ............................................................................................................................. 6
Executive summary.................................................................................................................... 7
1 Introduction........................................................................................................................ 8
   1.1 Starting point for the workshops ................................................................................. 8
   1.2 Facts and figures of the workshops ........................................................................... 11
2 Evaluation part of the CRISP Methodology: configuration and assessment............... 16
   2.1 General approach to the preparation for the workshops ........................................... 16
       2.1.1 Scenario preparation as part of the configuration stage............................. 19
       2.1.2 Exercise preparation as part of the assessment stage................................. 23
   2.2 The workshops as part of the assessment stage......................................................... 28
   2.3 Feedback from the workshop participants on the assessment exercise to learn from 31
   2.4 Main conclusion for the evaluation part of the CRISP Methodology and resulting recommendations................................................................................................................. 36
3 Certification part of the CRISP Methodology ................................................................. 38
   3.1 General preparation approach for the workshops ..................................................... 38
   3.2 The debate on the chosen main elements of the certification scheme ....................... 41
       3.2.1 Introduction to CRISP’s Methodology, its relation to the requirements of the S-T-E-Fi dimensions and the requirements for certification......................................................... 41
       3.2.2 Debate on the chosen main elements of the certification scheme and their specific issues................................................................................................................... 42
   3.3 Summarising the main conclusions and recommendations for the certification part of the CRISP Methodology ....................................................................................................................... 50
       3.3.1 Main conclusions........................................................................................... 50
       3.3.2 Main recommendations.................................................................................... 52
4 Conclusion based on the workshop outcomes ................................................................. 54
List of References .................................................................................................................... 57
LIST OF SELECTED ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCTV</td>
<td>Closed-circuit television</td>
</tr>
<tr>
<td>CEN</td>
<td>Comité Européen de Normalisation</td>
</tr>
<tr>
<td>CENELEC</td>
<td>Comité Européen de Normalisation Electrotechnique</td>
</tr>
<tr>
<td>CoESS</td>
<td>Confederation of European security services</td>
</tr>
<tr>
<td>DPAs</td>
<td>Data Protection Authorities</td>
</tr>
<tr>
<td>DEL</td>
<td>Deliverable report</td>
</tr>
<tr>
<td>DoW</td>
<td>Description of Work of the CRISP project</td>
</tr>
<tr>
<td>EN</td>
<td>European Norm</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IP-RS</td>
<td>Information Commissioner of the Republic of Slovenia</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>NEN</td>
<td>Netherlands Standardization Institute</td>
</tr>
<tr>
<td>PSS</td>
<td>Product – System – Service</td>
</tr>
<tr>
<td>R₁,R₂:</td>
<td>Output from one evaluation activity which work as input to another activity</td>
</tr>
<tr>
<td>RPAS</td>
<td>Remotely Piloted Aerial Systems</td>
</tr>
<tr>
<td>TRI</td>
<td>Trilateral Research &amp; Consulting</td>
</tr>
<tr>
<td>TRL</td>
<td>Technology Readiness Level</td>
</tr>
<tr>
<td>TUB-CTS</td>
<td>Technische Universität Berlin – Center for Technology and Society</td>
</tr>
<tr>
<td>TUB-INNO</td>
<td>Technische Universität Berlin – Chair for Innovation Economics</td>
</tr>
<tr>
<td>UJI</td>
<td>University Jaume I of Castellón</td>
</tr>
<tr>
<td>VICESSE</td>
<td>Vienna Centre for Societal Security</td>
</tr>
<tr>
<td>VUB</td>
<td>Vrije Universiteit Brussels</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
<tr>
<td>WP 1</td>
<td>Work Package on ‘Categorising Security Equipment, Systems and Services’</td>
</tr>
<tr>
<td>WP 2</td>
<td>Work Package on ‘Review of Standards, Certification and Accreditation for Security Products, Systems and Services’</td>
</tr>
<tr>
<td>WP 3</td>
<td>Work Package on ‘Security Certification Stakeholder Analysis’</td>
</tr>
<tr>
<td>WP 5</td>
<td>Work Package on the ‘Validated Certification Methodology’</td>
</tr>
<tr>
<td>WP 6</td>
<td>Work Package on ‘Developing a Roadmap’</td>
</tr>
<tr>
<td>WP7</td>
<td>Work Package on ‘Enhancing Confidence in the New Certification Measures’</td>
</tr>
</tbody>
</table>
LIST OF FIGURES

Figure 1: CRISP Evaluation and Certification Methodology .......................................................... 9
Figure 2: themes/scenarios of the series of scenario-based workshops ........................................... 12
Figure 3: country of origin of the scenario-based workshop participants (N=23) .......................... 13
Figure 4: exemplarily invitation for the drones workshop .............................................................. 14
Figure 5: rough agenda of the international and national scenario-based workshops .................. 15
Figure 6: proposed configuration and assessment stages during evaluation ............................... 16
Figure 7: basic information for the configuration set-up aspects (mock-up) ............................... 18
Figure 8: project set-up (mock-up) ............................................................................................. 19
Figure 9: questions on application area and function (mock-up) ............................................... 20
Figure 10: questions on technology specifications (mock-up) ..................................................... 20
Figure 11: questions on the technology specification (mock-up) ............................................... 21
Figure 12: configuration report R1 (mock-up) ............................................................................. 22
Figure 13: proposed evaluation criteria questioning (mock-up) ................................................. 23
Figure 14: four level structure of the S-T-E-Fi approach .............................................................. 24
Figure 15: short cuts of the evaluation criteria questionnaires ................................................... 27
Figure 16: exemplary section of the efficiency questionnaire for the Drones Workshop .............. 30
Figure 17: workshop exercise slide ........................................................................................... 30
Figure 18: response rate of the alarm systems/CCTV workshop participants ............................. 35
Figure 19: preparation process for the discussion of the certification part of the CRISP Methodology during the international scenario-based workshops ......................................................... 38
Figure 20: CRISP Methodology and its relation to the evaluation criteria and requirements for certification .......................................................................................................................... 41
Figure 21: the proposal of the CRISP consortium on the overall timeframe ............................... 49
Figure 22: draft version of the CRISP procedure presented at the Validation Workshop (September 2015) ........................................................................................................................................ 54
Figure 23: first refinement resulting in CRISP’s Evaluation and Certification Methodology as presented in CRISP report 5.1 (October 2015) ................................................................. 55
Figure 24: the modified and current CRISP Methodology ........................................................... 56
LIST OF TABLES

Table 1: external stakeholders participating at CRISP’s scenario-based workshops 1-4 ........ 13
Table 2: S-T-E-Fi criteria/attributes for the workshop on alarm systems/CCTV ............... 25
Table 3: numbers of stakeholders per dimension .............................................................. 28
Table 4: possible assessment findings reported in R2 – refinement .................................. 36
Table 5: the proposed context of the selected elements of the certification scheme .......... 39
Table 6: summary of reasons named by experts to choose Alarm Systems as an application area for the CRISP Certification Scheme ................................................................. 44
Table 7: the main recommendations on the discussed elements for CRISP certification ...... 52
EXECUTIVE SUMMARY

This report is the second and last deliverable for CRISP’s Work Package 5 (WP 5), ‘Validated Certification Methodology’. The objectives of this WP are as follows:

“To develop and describe a harmonised approach and certification methodology for security products and systems in Europe, to develop and outline policy and certification procedures for security certification, and to test drive the proposed certification model, evaluate its actual working and, accordingly, revise and refine the certification scheme”\(^1\).

The focus of this WP 5 report is on the documentation of four scenario-based workshops and its effect on the further project research. The starting point for these scenario-based workshops was the CRISP Methodology beforehand developed, which was presented in deliverable 5.1, the first deliverable report of WP 5. The scenario-based workshops aimed to test and discuss this CRISP Methodology in more detail with multifunctional stakeholders by using (real and fictional) case examples and different application areas such as drones, CCTV, border control security and furthermore a service offer for the application area of household security.

In conclusion, the stakeholder’s feedback was used for further validation activity and led to a refinement of the CRISP Evaluation and Certification Methodology. The refined methodology presented in this report serves as the basis for the forthcoming project research.

In more detail, this report is structured as follows:

**Chapter 1** gives a short introduction to the CRISP project, the methodological starting point and the basic conditions for the scenario-based workshops.

**Chapter 2** focuses on the evaluation part of the CRISP Methodology, and how it was tested during the scenario-based workshops. It also presents the feedback on the assessment exercise, and the main conclusions and recommendations for the upcoming project work drawn from them.

**Chapter 3** is devoted to the certification part of the CRISP Methodology, how it was presented during the scenario-based workshops and describes the main conclusions and recommendations to which the CRISP consortium has come regarding the upcoming project work.

**Chapter 4** illustrates the refinement of the CRISP Methodology based on the outcomes of the different workshop activities.

---

\(^1\) Description of Work (DoW) of the CRISP project, p. 15.
INTRODUCTION

The EU FP7 funded project “CRISP” (Evaluation and Certification Schemes for Security Products; Grant Agreement No: 607941) aims at facilitating a harmonised playing field in the European security industry by developing a robust methodology for security product certification. To achieve the most optimal solution approximately possible, CRISP will enhance existing security evaluation and certification schemes by offering certification based on a four-dimensional approach. In this connection, it was required from the very beginning of the project to cover a wide breadth of existing equipment, and to consider not only security products and systems certification, but also to take into account security service certification. Thus, up to now, the focus was on security products, systems and services (PSS) evaluation and certification.

A first evaluation and certification draft was developed from June to August 2015 by the CRISP consortium, which was presented to a variety of stakeholder groups at the CRISP Validation Workshop in September 2015 (see Figure 22 presenting the graphical presentation of the first draft of the CRISP Methodology, p. 54). At this workshop, the presented draft methodology was discussed in order to receive direct feedback from different stakeholders’ perspectives and to ensure stakeholder involvement from the earliest possible date of the developmental stage of the methodology. The feedback and the recommendations expressed by the stakeholders during this first CRISP workshop were used for a first refinement of CRISP’s Evaluation and Certification Methodology which was finally presented in the deliverable report of WP 5 in October 2015 (hereafter entitled CRISP report 5.1). This two-part methodology was then the starting point for the ensuing scenario-based workshops.

1.1 STARTING POINT FOR THE WORKSHOPS

The assessment of legal, ethical and, in the broader sense, social and political implications has notably been attracting interest within the European security research in recent years. Valuation methods like Privacy Impact Assessment or Social Impact Assessment particularly enforce claims of accompanying the development of technology within the

---

2 Such as: end-users from the security industry, standardisation, certification and accreditation bodies, Federal Ministry and public administration as well as researchers and academics in the field of security, social science, law and ethics.


meaning of risk assessment. Their initial point is the observation that numerous security solutions have an immediate impact on the configuration of contexts in the realms of life, which applies to social, economic, legal, or individual aspects altogether.

As seen in Figure 1, the overall CRISP Methodology was developed by the CRISP consortium and presented in CRISP report 5.1\(^6\). CRISP’s approach is firstly composed of an evaluation part consisting of two main stages (configuration and S-T-E-Fi assessment) and secondly of a certification part as third-party attestation related to products, processes, systems or persons\(^7\), consisting of two stages (audit\(^8\) and attestation\(^9\)). The certification part considers the results of the evaluation part. This two-part methodology emerged during the research work of the CRISP project taking into account existing evaluation and certification processes and expert recommendations of several validation activities.\(^10\)

**Figure 1: CRISP Evaluation and Certification Methodology**


As described in the first WP 5 report, the evaluation part of the CRISP Methodology is participatory, systematic, and iterative by nature, enabling the determination, selection, and assessment of security PSS according to the four S-T-E-Fi dimensions.\(^11\) S-T-E-Fi is an approach that stands for Security, Trust, Efficiency, and Freedom infringement, which aims to systematise assessment dimensions in order to increase the level of inter-subjectivity

---

\(^6\) Hempel, et al., op cit., October 2015.

\(^7\) According to ISO/IEC 17000:2004 *Conformity assessment - Vocabulary and general principles*.

\(^8\) Audit: systematic, independent, documented process for obtaining records, statements of fact or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled according to ISO/IEC 17000:2004 *Conformity assessment - Vocabulary and general principles*.

\(^9\) Attestation: issue of a statement, based on a decision following review, that fulfilment of specified requirements has been demonstrated according to ISO/IEC 17000:2004 *Conformity assessment - Vocabulary and general principles*.

\(^10\) Hempel, et al., op cit., October 2015, p. 42.

during an assessment process.\textsuperscript{12} In this context, the aim is to integrate complex and multidimensional relationships into one approach which does not mutually exclude the above mentioned single perspectives of security, trust, efficiency, and freedoms but rather unites them in a systematic and systemic approach, by furthermore allowing to uncover potential conflicts between them. As the identification of conflicts is based on impact matrices (for further explanation see CRISP report 5.1, chapter 6.1), some individual features of the procedure follow the method of Quality Function Deployment (QFD). The QFD procedure, developed in the late 1960s, is an approach for quality assurance that involves the determination of ‘customer’\textsuperscript{13} needs and requirements. These customer needs and requirements shall help to put a solution (in the sense of a new product) directly into practice of development.\textsuperscript{14} Therefore, it is the objective of this systematic QFD method to ensure that important elements of a solution are determined by the identified customer requirements. The identified customer needs are summarised in a table form and transmitted into a correlation matrix (QFD matrix). The QFD matrix structure allows a pairwise comparison of the relations for which different solution characteristics (positive, negative, neutral) can be defined, based on existing rules. Arising conflicts to be seen from the QFD matrix can then be solved by allowing compromises between the identified customer needs and requirements.

Coming back to the CRISP project, the S-T-E-Fi approach as one essential element of the evaluation part and hence for the certification part of the CRISP Methodology however, “attempts to systematise assessment dimensions by encompassing as many perspectives as possible in an easily comprehensible manner, which allows the integration of different perspectives and activities into one approach and thus increases the level of inter-subjectivity during an assessment process.\textsuperscript{15} Implementing the S-T-E-Fi approach into the CRISP methodology shall help to avoid acceptance problems that challenge current certification schemes by offering certification applicants to go beyond usual self-assured methods of simplification and confronting them with complexity and possible effects that a security PSS might have in the S-T-E-Fi context.”\textsuperscript{16}

Since CRISP is using a participatory, cross-stakeholder and scenario-based approach, CRISP is going far beyond this previous described QFD method.

\begin{itemize}
  
  \item \textsuperscript{13} ‘Customer’ in the context of QDF means “external customer” in terms of buyer, as well as everyone involved in the implementation process (“internal customer”). The term ‘customer’ is not used in the CRISP context up to this point.
  
  \item \textsuperscript{14} Herzwurm, Georg, „Was ist QDF?“ QDF Institut Deutschland e.V., 2008. http://www.qfd-id.de/wasistqfd/index.html.
  
  \item \textsuperscript{15} Hempel, et al., op. cit., 2013, p. 748.
  
  \item \textsuperscript{16} Hempel, et al., op cit., October 2015, p. 1.
\end{itemize}
“The evaluation part of the CRISP methodology is participatory, systematic, and iterative by nature enabling the determination, selection and assessment of security PSS according to the four S-T-E-Fi dimensions. It is participatory due to the encouragement of an (early) involvement of different stakeholders. It is systemic as a variety of differently-dimensional criteria will be brought into a matrix structure. And it is iterative as the evaluation process is repeated until each potential conflict uncovered is addressed to relevant / involved stakeholders and, where appropriate solved.”

In order to reflect potentially varying needs of the users, producers and assessors involved in the application of security solutions in practice, and to test the evaluation and certification methodology, a series of scenario-based workshops were scheduled in the course of the CRISP project by inviting multifunctional stakeholders. Following the two-part structure of the methodology, the workflow and the output of these workshops will be presented below by starting with an overview of the facts and figures of the scenario-based workshops first.

1.2 FACTS AND FIGURES OF THE WORKSHOPS

A stated goal of the CRISP project is to foster and promote stakeholder involvement from the very beginning for a greater acceptance and usability of the developed approach. In total, four workshops have been scheduled and conducted with external stakeholders in order to test the CRISP Methodology based on four different scenarios/themes. Considering the taxonomy created in CRISP’s WP 1 and previous research work, the following application areas have been chosen (see also Figure 2):

- Workshop 1: scenario on border control security
- Workshop 2: scenario on drones
- Workshop 3: scenario on alarm systems/CCTV
- Workshop 4: scenario in the application area of household security.

As the CRISP project, up to this point, addressed security products, systems and services across different application areas such as ‘border management’, ‘security of the citizens, ‘critical infrastructure’ and so forth, it was envisaged to cover a broad variation of topics. It

17 Hempel, et al., op cit., October 2015, p. 61.
18 See “Participation of stakeholders” (p. 21) DoW of the CRISP project.
19 This refers to the case studies on alarm systems, CCTV and drones (including contacts to external stakeholders obtained) done in CRISP’s WP 4 and presented in CRISP report 4.3. Published in Kamara, Irene, Paul de Hert, Rosamunde van Brakel, Ioulia Konstantinou, Alessia Tanas, Simone Wurster, Tim Pohlmann, Nathalie Hirschman, Leon Hempel, Barbara Bossert, Cristina Pauner, Jorge Viguri, Artemi Rallo, Rosario Garcia, Reinhard Kreissl, Florian Fritz, Roger von Laufenberg, “S-T-E-Fi based SWOT analysis of existing schemes”, DEL 4.3 CRISP Project, 30 June 2015.
20 For workshop 1 and 4: contacts with the relevant institutions made it possible to win the external stakeholders for the workshops.
21 See for example Sveinsdottir, Thordis, Rachel Finn, Rowena Rodrigues, Kush Wadhwa, Florian Fritz, Reinhard Kreissl, Roger von Laufenberg, Paul de Hert, Alessia Tanas, and Rosamunde van
is a distinctive feature and a great opportunity for the CRISP project that real case scenarios and related external stakeholders could be won for the national workshops 1 and 4. This means that the scenario and the associated system or service dealt with had been tested on the market or is in use already. Concerning this matter, anonymity of the real case scenarios within the national workshops was a necessity to guarantee. Hence, the scenario description in this report in chapter 2.2.1 is very limited. To guarantee anonymous use of the provided content is a well-established practice in empirical social research and, amongst other reasons, aims at preventing damage of all parties involved.22

Figure 2: themes/scenarios of the series of scenario-based workshops
Source: @Hirschmann, January 2016.

As a consequence, the contents of the scenarios for the workshops 2 and 3 were targeted at an international audience with international stakeholders (hereinafter entitled 'international workshops'), those of the workshops 1 and 4 at a national audience with German stakeholders (hereinafter entitled 'national workshops'). Even though the number of external attendees differed as seen in Table 1, the total number of participants for each workshop corresponded to the planned workshop size. One crucial point for the preparation of the workshops regarding the evaluation part was to have expertise – in form of external stakeholders – on all S-T-E-Fi dimensions available. This condition was met for each scenario-based workshop as seen in Table 3 on page 28. Furthermore, the maximum number of ten external stakeholders was not to be exceeded to maintain a good and valuable working environment. In total, 23 stakeholders, CRISP consortium partners not included, from seven European countries (see Figure 3, p. 13) attended the four workshop events, forming different player groups such as

---

22 See confirmation in the DoW of the CRISP project, chapter 4 on “Ethics issues”. Or for instance the basic principle of “Damage Prevention” (Hopf, Christel, “Forschungsethik und qualitative Forschung”. In: Flick, Uwe, Kardorff, Ernst von & Steinke, Ines (Hg.), Qualitative Forschung. Ein Handbuch. Reinbek bei Hamburg: Rowohlt Taschenbuch Verlag, 2009, p. 594). Or other ethical principles promoted by the German Sociological Association. This basic principle of “Damage Prevention” indicates that nobody who is involved in empirical research shall suffer disadvantages and damages due to his or her participation.
certification and standardisation body representatives, end-users\textsuperscript{23}, researchers, and academics. This also included two Advisory Board members of the CRISP project.\textsuperscript{24}

### Table 1: external stakeholders participating at CRISP’s scenario-based workshops 1-4

<table>
<thead>
<tr>
<th>Number of stakeholders</th>
<th>workshop 1</th>
<th>workshop 2</th>
<th>workshop 3</th>
<th>workshop 4</th>
<th>workshops 1-4</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-users</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Manufacturer/producer/vendor</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Certification body/standardisation body/ accreditation body</td>
<td></td>
<td>3</td>
<td></td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DPA/jurisdiction/lawyer/expert on law</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field researcher/academic</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Other organisations/institutions</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td><strong>In total</strong></td>
<td><strong>4</strong></td>
<td><strong>7</strong></td>
<td><strong>8</strong></td>
<td><strong>4</strong></td>
<td><strong>23</strong></td>
</tr>
</tbody>
</table>

### Figure 3: country of origin of the scenario-based workshop participants (N=23)

Note: only external participants. Source: own presentation. Map of Europe: https://commons.wikimedia.org/wiki/File%3ABlank_map_of_Europe.svg

\textsuperscript{23} End-users attending the workshops: operators working with security products, systems and services, such as representatives of local authorities.

\textsuperscript{24} Two of the Advisory Board members also attended the Validation Workshop in September 2015. The Advisory Board is a group of important security and certification stakeholders. Currently, there are five experts on the CRISP Advisory Board representing: materials research testing and certification, testing and evaluation of security products, aviation security, and security manufacturers. An Advisory Board with relevant expertise was incorporated right from the project’s beginning with members reflecting a range of expertise and interests – scientific, technical, academic, standards setting, ethical, and so forth. The Advisory Board supports the project to guarantee both scientific excellence and policy relevance of the project.
The coordination, including establishing contact to the relevant stakeholders, the preparation and performance was divided among the CRISP partners. The national workshops were moderated by Leon Hempel and Nathalie Hirschmann (CRISP partners from TUB-CTS). Tatsiana Haponava (CRISP partner from NEN) was chair of the international workshops, supported by Nathalie Hirschmann (TUB-CTS).

Figure 4: exemplarily invitation for the drones workshop
Source: @Sveinsdottir, Pauner-Chulvi, Burnik, and Kamara, October 2015.

All workshops were planned as half-day events at the Center for Technology and Society, located at Technische Universität Berlin (TUB-CTS). The first national workshop was held on the 29th of September 2015, the two international ones in November 2015 on the 25th and the 26th and the last national workshop was conducted on the 3rd of December 2015.

Following the two-part structure of the CRISP Methodology as described before, the national and international workshops had slightly different foci, which had small effects on the workshop preparation and the agenda setting: the national workshops were mostly focused on the evaluation part, whereas the international workshops focused more on debating about the outcome of the certification part, as more experts on certification and standardisation were attending. Although the different weighting of the evaluation and certification part within the
workshops was seen as most viable for the conclusions regarding the methodology, in all four workshops, however, the exercise for the evaluation part of CRISP’s Methodology was performed (see chapter 2.2 of this report). Regardless of the different foci, all workshops started with a short introduction into the CRISP project and the CRISP Methodology, followed by a practical testing of the evaluation part, including a first feedback round on the stakeholders’ impressions.

Figure 5: rough agenda of the international and national scenario-based workshops

The workshop preparations made for the evaluation and certification part of the CRISP Methodology will be individually explained in the relevant chapters of this report: this contains the preparations for the evaluation part in chapter 2 and for the certification part in chapter 3. The consequential conclusions for the overall methodology can be found in chapter 4 of this report.
2 EVALUATION PART OF THE CRISP METHODOLOGY: CONFIGURATION AND ASSESSMENT

2.1 GENERAL APPROACH TO THE PREPARATION FOR THE WORKSHOPS

As described in CRISP report 5.1, chapter 6.1 and illustrated in Figure 6, the first part of CRISP’s Methodology involves two stages which cover the first two functions of certification as defined by ISO/IEC 17067:201325: a configuration stage and an assessment stage. These two stages as illustrated in Figure 6, were introduced and explained during the workshops.26

![Figure 6: proposed configuration and assessment stages during evaluation](source)

Source: Hempel, et al., op. cit., October 2015, p. 43.

---


26 Although the workshop language in the national workshops was German, a translation of the presented material was not seen necessary. None of the workshop participants addressed upcoming language issues in the feedback session.
Both stages demand stakeholder involvement and need reflection by different actor roles. In CRISP report 5.1, three main actor roles named “project leader”, “project participants” and “information provider”, were introduced.

For more information on the main actor roles and their functions, please read the box below.

Retrospection to “Actor Roles and Functions” (Hempel, et al., op. cit., October 2015, pp. 49f)

1. ‘Project leader’: acts as a coordinator within the whole evaluation process providing all relevant information regarding a security PSS. The ‘project leader’ must be capable of giving a review of the security PSS objectives as well as general and specific information. This could be, a manufacturer or supplier of a security PSS – eventually a purchaser in case of new security PSS.

2. ‘Project participants’: are involved in the assessment stage once invited by the ‘project leader’. There are different stakeholder groups such as presented in Table 7 (no exhaustive list). The group of ‘project participants’ can, for instance, consist of manufacturers or suppliers, (end-)users or purchasers, or other (professional) parties interested or affected by a security PSS such as NGO’s, data protection experts, politicians.

3. ‘Information provider’: in case configuration questions and assessment criteria questions cannot be answered exclusively and / or adequately, a ‘project leader’ / ‘project participant’ shall be able to consult third persons’ both for the configuration and assessment stage (see actor role functions in Table 8).

Table 8: Intended actor roles and functions during evaluation

<table>
<thead>
<tr>
<th>actor roles</th>
<th>function</th>
<th>involved in</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘project leader’</td>
<td>• set up a new (application) scenario (including general information, technology specifications</td>
<td>configuration &amp; assessment</td>
</tr>
<tr>
<td>(coordinator)</td>
<td>• specify and invite other stakeholders relevant for the assessment stage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• answer configuration questions and evaluation criteria questionnaire</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• provide evidence (such as standards or other forms of certifications) when requested</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• delegate questions to an ‘information provider’ (for verification)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• access to evaluation outputs: $R_1$ and $R_2$ (both versions)</td>
<td></td>
</tr>
<tr>
<td>‘project participants’</td>
<td>• access to application scenarios (once invited by the ‘project leader’)</td>
<td>assessment</td>
</tr>
<tr>
<td></td>
<td>• answer the evaluation criteria questionnaire</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• consult ‘information provider’ for evaluation criteria questionnaire</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• access to evaluation outputs: $R_1$ and $R_2$ (primarily Partial Evaluation Report)</td>
<td></td>
</tr>
<tr>
<td>‘information provider’</td>
<td>• answer only the configuration questions which have been delegated by the ‘project leader’</td>
<td>configuration</td>
</tr>
<tr>
<td></td>
<td>• if applicable, access to evaluation output: $R_1$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• answer only those questions of the evaluation criteria questionnaire which have been</td>
<td></td>
</tr>
<tr>
<td></td>
<td>delegated by the ‘project leader’ and / or ‘project participants’</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• if applicable, access to evaluation outputs: $R_1$ and $R_2$ (primarily Partial</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Evaluation Report)</td>
<td></td>
</tr>
</tbody>
</table>
Before a CRISP certification can take place, applicants for certification need to apply for the CRISP evaluation procedure first by providing general information on their security PSS as intended in CRISP report 5.1, chapter 6.1.1 in the first stage of configuration (see also Figure 7). This first stage is then followed by the assessment stage which aims to evaluate a security PSS by using an assessment questionnaire (entitled in CRISP report 5.1: “evaluation criteria questionnaire”\textsuperscript{27}).

\textbf{Figure 7: basic information for the configuration set-up aspects (mock-up)}

Source: @Hirschmann, September 2015; Hempel, et al., op. cit., October 2015, p. 44f.

The preparations for the evaluation part prior to the workshops were extensive and consisted of two main tasks: first the preparation of the scenario as part of the configuration stage, which served as the starting point at the actual workshops, and second the preparation of the assessment exercise as part of the assessment stage.

\textsuperscript{27} Hempel, et al., op. cit., October 2015, p. 46.
2.1.1 Scenario preparation as part of the configuration stage

2.1.1.1 National workshops

In preparation for the national workshops, the person in charge or ‘project leader’ was contacted and invited for the CRISP event by the CRISP partners from TUB-CTS. After the invitation was accepted, information regarding the specification of the security functionalities, the purpose and the technological specifications (as far as possible and applicable), the stakeholders involved, and the context in which the system or service is used, was obtained. The workshop organisers from TUB-CTS explicitly asked their first contact person to forward the workshop invitation to additional stakeholders considering the S-T-E-Fi dimensions. Once all confirmed participants were reported to the organisers, the attendees were allocated to one or more S-T-E-Fi dimensions up front.

The preparation process for the configuration stage is explained in the following mock-up presentation.

![Project set-up (mock-up)](image)

**Figure 8: project set-up (mock-up)**

Source: @Hempel, September 2015.
Figure 9: questions on application area and function (mock-up)
Source: @Hempel, September 2015.

Figure 10: questions on technology specifications (mock-up)
Source: @Hempel, September 2015.
The closing of the configuration stage stipulates a first output (R1), a summary of all basic information which works as input for the assessment stage and as an information source for the ‘project participants’ once they are invited (see mock-up Figure 12).

Following this procedure, a short summary of the scenarios for workshop 1 and workshop 4 is presented in the boxes below.

**THE SCENARIO FOR WORKSHOP 1 ON BORDER CONTROL**

*Scenario: automated border control when entering a country*

(Compressed explanation due to anonymity reasons. The system was familiar to all external stakeholders.)

The management of increasing passenger volume is to be improved by implementing an automated border control system. As the service (check) is done automatically, field service staff can be released from work in order to increase security elsewhere. No additional data are to be collected by using the system, but information specified in the passport will be compared to the data stored in the police database. By implementing the system, it is aimed to increase and ease the service quality for travelers as well as increase security.

---

The topic of this workshop was an evaluation and certification procedure in the context of safer living and house building construction which aims at increasing security and safety issues as well as trust components, such as reducing fear of crime by habitants, while also taking into account efficiency aspects and personal rights on a very basic level.

**THE SCENARIO FOR WORKSHOP 4 ON SAFER LIVING**

*(Compressed explanation due to anonymity reasons. The service was familiar to all external stakeholders.)*

The topic of this workshop was an evaluation and certification procedure in the context of safer living and house building construction which aims at increasing security and safety issues as well as trust components, such as reducing fear of crime by habitants, while also taking into account efficiency aspects and personal rights on a very basic level.

**Figure 12: configuration report R₁ (mock-up)**

Source: @Hempel, September 2015.

### 2.1.1.2 International workshops

The preparation of the two international workshops was provided by a group of CRISP consortium partners who defined the application area and generated the relevant scenario to be assessed during the workshops. CRISP partners from TRI, UJI, IP-RS and VUB acted as ‘project leader’ for workshop 2 on drones and CRISP partners from TUB-INNO, NEN and VICESSE acted as ‘project leader’ for workshop 3 on alarm systems/CCTV together with the technology provider. This procedure was considered necessary in order to find out whether the requirements on a ‘project leader’ were communicated effectively and whether the information about a security PSS and the scenario provided to ‘project participants’ as assessors were adequate enough to take part in the *assessment* stage in case the security PSS is not familiar to them. This will also become important for certification bodies using the CRISP Evaluation and Certification Methodology for the upcoming CRISP research work.
The ‘project leaders’ of each workshop invited relevant external stakeholders in relation to either drones or alarm systems/CCTV. Again, it was emphasised to have experts on all S-T-E-Fi dimensions available during the workshops. The presentation of the scenarios for workshop 2 and workshop 4 was an agenda item and hence will be displayed in chapter 2.2 of this report.

2.1.2 Exercise preparation as part of the assessment stage

As described in CRISP report 5.1, a security PSS shall be assessed with the help of the S-T-E-Fi approach by using an evaluation criteria questionnaire.

“The evaluation criteria questionnaire not only aims towards acquiring information on a specific use case of a security PSS. It also helps to identify interrelations and uncover potential conflicts within or between S-T-E-Fi criteria – and hence between different stakeholders and social groups.”

In order to test this ‘dimension-criteria-attributes approach’ practically as presented in CRISP report 5.1 and as shown exemplarily in Figure 13, the approach structure needed to be translated into a questionnaire format to be filled in by the workshop attendees.

Figure 13: proposed evaluation criteria questioning (mock-up)
Source: Hempel, et al., op. cit., October 2015, p. 46.

As introduced in CRISP report 5.1, the S-T-E-Fi approach follows a four level structure as seen in Figure 14. The assessment exercise focused mainly on the yes/no questions related to attributes (hereinafter entitled associates attribute questions). As the exercise was envisaged

---

29 Hempel, et al., op. cit., October 2015, p. 46.
for all four workshops, S-T-E-Fi criteria and associated attribute questions needed to be compiled on the basis of the criterion catalogue that was produced in the context of CRISP WP 4 in relation to the topic treated. They then were translated into four questionnaires; one questionnaire for each dimension. This preparation was executed for all four workshops.

![Figure 14: four level structure of the S-T-E-Fi approach](source: Hempel, et al., op cit., October 2015, p. 29.)

With reference to the applicability, there was a slight difference in the number of S-T-E-Fi criteria and associated attributes between the workshops. Table 2 illustrates exemplary criteria and associated attributes used for the Alarm Systems/CCTV workshop and offers a preparatory look at the debate about the defined scope of the CRISP Certification Scheme (see chapter 3.2.2 and 3.3). To keep the workshops easily manageable and cost-effective for both the CRISP consortium and the workshop participants, the questionnaires were converted in an online survey format and (portable) prepared computers were provided on site. Figure 15 on page 27 illustrates some short cuts of the questionnaires format.

---

<table>
<thead>
<tr>
<th>Security criteria</th>
<th>Security attributes for alarm system</th>
</tr>
</thead>
</table>
| 1 risk classification | allowance risk classification  
need_risk classification |
| 2 profiling        | profiling  
need_profiling |
| 3 data matching    | database matching  
third party database matching  
need_database matching |
| 4 data security    | data transmission to third parties  
authentication |
| 5 sensitivity      | sensitivity tests  
false positive rate  
false negative rate |
| 6 improved safety  | before/after comparison |
| 7 robustness       | manipulation |
| 8 reliability      | circumvention |

<table>
<thead>
<tr>
<th>Trust criteria</th>
<th>Trust attributes</th>
</tr>
</thead>
</table>
| 1 visibility   | openness_visibility  
openness_transparency  
signage |
| 2 exposition   | focus / target group / end user  
system  
operators  
users |
| 3 user-related information | run-up  
user groups  
appropriateness  
alarm results |
| 4 user-related transparency | false alarms |
| 5 perception   | wellbeing |
| 6 operator-related information | manual |
| 7 operator competence | training  
training_awareness |
| 8 work environment | working conditions |
| 9 observability | nakedness |
| 10 transparency | complaint mechanism |
| 11 safety       | hazard |

<table>
<thead>
<tr>
<th>Efficiency criteria</th>
<th>Efficiency attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 accountability</td>
<td>accountability</td>
</tr>
<tr>
<td>2 interoperability</td>
<td>interoperability</td>
</tr>
<tr>
<td>3 energy efficiency</td>
<td>energy efficiency</td>
</tr>
<tr>
<td>4 ergonomics</td>
<td>usability</td>
</tr>
</tbody>
</table>
| 5 life cycle costs  | usability  
usability_evidence |
| 6 maintenance costs | footprint |
| 7 malfunction       | protective measures  
protective measures_provided |
| 8 misuse            | protective measures  
protective measures_provided |
| 9 privacy           | protective measures  
protective measures_provided |
<p>| 10 process continuity | operational life |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>process organisation</td>
<td>technical updates and upgrades</td>
</tr>
<tr>
<td>12</td>
<td>usability</td>
<td>technology development</td>
</tr>
<tr>
<td>13</td>
<td>versatility</td>
<td>usability</td>
</tr>
<tr>
<td></td>
<td><strong>Freedom infringement criteria</strong></td>
<td><strong>Freedom infringement attributes</strong></td>
</tr>
<tr>
<td>1</td>
<td>automated decision making</td>
<td>profiling</td>
</tr>
<tr>
<td>2</td>
<td>due process</td>
<td>access to material</td>
</tr>
<tr>
<td>3</td>
<td>personal data</td>
<td>processing of personal data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>fairness</td>
</tr>
<tr>
<td></td>
<td></td>
<td>processing purposes (finality)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>proportionality</td>
</tr>
<tr>
<td></td>
<td></td>
<td>data security - human resource security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>lawfulness (legal grounds)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sensitive personal data</td>
</tr>
<tr>
<td>4</td>
<td>data security</td>
<td>restrictions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>transfer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>data protection impact assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>operations security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>communications security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>system acquisition, development and maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>supplier relationships</td>
</tr>
<tr>
<td></td>
<td></td>
<td>information security incident</td>
</tr>
<tr>
<td></td>
<td></td>
<td>authorisation</td>
</tr>
<tr>
<td>5</td>
<td>presumption of innocence</td>
<td>evidence_image</td>
</tr>
<tr>
<td></td>
<td></td>
<td>evidence_sound</td>
</tr>
<tr>
<td>6</td>
<td>prevention of discrimination</td>
<td>equal treatment</td>
</tr>
<tr>
<td>7</td>
<td>privacy</td>
<td>privacy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Legality</td>
</tr>
<tr>
<td></td>
<td></td>
<td>legitimacy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>proportionality</td>
</tr>
<tr>
<td>8</td>
<td>retention</td>
<td>retention</td>
</tr>
<tr>
<td></td>
<td></td>
<td>retention_safeguards</td>
</tr>
</tbody>
</table>
Figure 15: short cuts of the evaluation criteria questionnaires
After the workshop attendees confirmed their workshop participation, they were allocated to at least one of the S-T-E-Fi dimensions, as seen in Table 3, in advance. The allocation was based on the respective expertise of the workshop participants.

<table>
<thead>
<tr>
<th>Table 3: numbers of stakeholders per dimension</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
</tr>
<tr>
<td>-------------------------</td>
</tr>
<tr>
<td>workshop 1</td>
</tr>
<tr>
<td>workshop 2</td>
</tr>
<tr>
<td>workshop 3</td>
</tr>
<tr>
<td>workshop 4</td>
</tr>
</tbody>
</table>

### 2.2 The Workshops as Part of the Assessment Stage

As explained before, the application area and the scenarios for the workshops were configured beforehand: either by CRISP consortium partners for the international workshops or by external stakeholders who acted as real ‘project leaders’ for the PSS subject of the national workshops. The scenario for the two national workshops was fixed, already well known by the invited stakeholders and hence did not cause any inquiries. However, a short summary was provided.

In contrast, during both international workshops two scenarios each were pictured to the stakeholders, of which one was selected by the attending external stakeholders. The boxes below illustrate the prepared scenarios presented to the audience. Finally, the participants in the Drones workshop voted for scenario 1 (“monitoring large events”) as it was perceived as more complex while still presenting considerable privacy and freedom infringement issues. The participants in the Alarm System/CCTV workshop voted for scenario 2 (“surveillance system placed in a more open environment”) as more privacy impacts had been noticed.

### The Scenarios for Workshop 2 on Drones

**Scenario 1: monitoring large events**

The organisers of an outdoor concert have contracted a drone operator to fly above the concert to monitor the crowd for purposes of safety and security as well as with the intention of using footage for publicity purposes. Attendees of the event were informed of the filming via a short notification in the terms and conditions statement when they bought their tickets online. The RPAS is equipped with video and photo camera, microphone and night vision capabilities. The images and sounds will be handed over to the organisers of the concert for distribution on the internet and social media.

**Scenario 2: search for lost persons**

Emergency services deploy an RPAS equipped with thermal imaging, a mobile phone signal sensor and GPS capabilities to search for hikers lost in the woods. The search picks up mobile phone and heat signatures from a number of hikers and campsites, generating “false alarms” which must be investigated by matching phone signals to individual mobile
THE SCENARIOS FOR WORKSHOP 2 ON DRONES

Phone accounts. The correct lost hikers are found after a few hours, and the data from the “false alarms” are immediately discarded.

THE SCENARIOS FOR WORKSHOP 3 ON ALARM SYSTEMS/CCTV

The scenarios for this workshop were based on a surveillance and tracking system of a notable institute for system technology. The surveillance system provides automatic approaches for video analysis and surveillance assistance. In a decentralised, sensor independent environment, the system is able to automatically detect abnormal behaviour or track suspicious persons. The operator of the system is on demand only if suspicious or critical situations appear.

Scenario 1: surveillance system placed in a closed environment

Bob enters an innovations research facility, as he has a meeting with Alice, located on the 6th floor. At the reception, Bob’s name and destination is entered into the surveillance system and linked with a picture of him taken by the CCTV located above the reception. Lastly, Bob receives an ID with his photograph on it and can finally take the elevator in order to meet Alice.

On his way, Bob is monitored by the surveillance system in the background, which has calculated the possible directions from the reception to Alice’s office and checks from time to time if Bob is going the right route. Only if Bob does not arrive at Alice’s office or enters restricted areas of the building – the research laboratories –, the surveillance system will inform the reception about Bob’s whereabouts. If Bob arrives at Alice’s office, the reception receives a short notification and the surveillance activity is terminated.

Scenario 2: surveillance system placed in a more open environment

Alice is at the hospital for a routine check and on her way to the 4th floor where the general practitioner is located. On the staircase to the 2nd floor however, Alice starts to feel dizzy and faints before she has the time to find a chair to sit down. The surveillance system, connected to the CCTV camera in the staircase, notices the strange behaviour of Alice and gives the reception a notification of a strange behaviour happening in the 2nd floor. At the reception, the operator decides what action is taken after matching the notification of the surveillance system with the actual footage of the CCTV camera.

Within all scenario-based workshops, the external workshop participants were instructed to act in the role of a ‘project participant’ at the assessment exercise. The actor role of an ‘information provider’ in person was not designed for the workshops. Instead, the availability of this potential role was indicated by the option “consult” as part of the assessment questionnaire (see red mark in Figure 16).
Figure 16: exemplary section of the efficiency questionnaire for the Drones Workshop

As illustrated in Figure 17, the attendees alias ‘project participants’ were asked to complete the respective S-T-E-Fi questionnaire alone. Once the exercise was understood, it started.

Figure 17: workshop exercise slide

Source: @Hirschmann, September 2015.
The respondents were allowed to select ‘consult’ in case they could not answer an evaluation criterion question appropriately. As this was a simulation, choosing this answer had no consequence (apart from telling the consortium that the question was not answerable by the respondent).

2.3 **Feedback from the Workshop Participants on the Assessment Exercise to Learn From**

For the evaluation part of the CRISP Methodology it was aimed foremost to find out:

- whether the information about a security PSS and the scenario provided to ‘project participants’ as assessors are adequate enough to take part in the *assessment* stage (especially in the case they do not know the security PSS),
- whether there were difficulties received during the assessment exercise.

The feedback provided during the scenario-based workshops was collected and categorised in the following sub-items in order to reveal what could be learned from the workshops.

1. **Distinction between the two parts of the CRISP Methodology**

   **To be learned from the workshops:**
   The evaluation part is the primary stage for certification which does not lead to a CRISP certificate or is attestation in the common sense. For the upcoming CRISP Roadmap and the Certification Manual (WP 6), a clear distinction between the evaluation and the certification part of the Methodology will be provided. This also refers to the wording used within each stage. For instance, the term “conflict score”, as introduced in the CRISP report 5.1 to be included in an Overall Evaluation Report (R2) is misleading and hence will not be used any longer in this context.

2. **Wording, language and terms used in the questionnaire (assessment exercise):**

   **To be learned from the workshops:**
   Some stakeholders from the national workshops pointed to a unique question wording by using careful question sequences, for example questions with “and”; “or”: “…recognisable and comprehensible...”; “Is xyz on the basis of the system or the ...” as there is room for interpretation (if one aspect is wrong, is the whole question to be considered as wrong?). As explained in chapter 2.1.2, the questionnaires focused more on the yes/no questions related to attributes. The note by the workshop moderators in both, the national and international workshops, stating that a qualitative response can be generally given to each yes/no question was
supported by the participants, as it allows concrete explanation and helps to reduce misinterpretations.\textsuperscript{31} Some of the workshop attendees recommended investing more effort into providing a clearer language of the assessment questions. This seemed to depend on the respective dimension, as others had no corrections to make regarding the language (the feedback that was given stated that for example the questions for the T dimension were ‘easy to understand’). Some of the stakeholders expressed the need for an explanation of certain terms used within questions, such as ‘controller’ or ‘user of a security PSS’, and to clearly distinguish between ‘system’ and ‘process’.

3. Evaluation Report (R\textsubscript{1}):

As the scenarios to give participants something to work with were created beforehand, the configuration stage in the workshops was omitted.

To be learned from the workshops:

The scenarios have to contain a certain level of information in order to be assessable. Therefore, substantial information has to be provided and concrete examples are needed. Otherwise, stakeholders are going to choose the option to consult an expert more often than it would be feasible. It seems to be a good option to clarify some of the more elaborated questions in the configuration stage already (E.g.: Are data being processed without the knowledge of an involved party? Is there Human-Machine interaction taking place?). As described in CRISP report 5.1, chapter 6.1.1, a first Evaluation Report (R\textsubscript{1}) summarises the main information including the technical components provided by an applicant (‘project leader’) and therefore serves as the basis for the assessment stage in which ‘project participants’ are to answer the evaluation criteria questionnaire relevant to the security PSS. This was not sufficient enough for the two international workshops, as participants reported difficulties in answering the questionnaires based on the information they got from the ‘project leader’. Confidentiality will be required from all parties involved in the assessment process.

As a consequence, R\textsubscript{1} is necessary for unknown and/new security PSS especially as it will allow for a better response of stakeholders in the role of ‘project participants’ to the asked evaluation criteria questionnaire. This became obvious through the observation that answering the evaluation criteria questionnaires by ‘project participants’ familiar with the presented PSS/scenarios was not reported as an issue. In any cases, confidentiality has to be a requirement for all parties involved.

\textsuperscript{31} As introduced in CRISP report 5.1 (p. 46), the yes/no as well as the qualitative questions are essential for the identification of interrelations within and between S-T-E-Fi criteria to be documented in the Overall Evaluation Report R\textsubscript{2}.
4. Evaluation criteria/practicality:

To be learned from the workshops:

Although the workshops did not serve as the validation activity for the evaluation criteria itself listed and defined in CRISP report 4.3, some remarks have been made. For instance, the evaluation criteria are “too societal” when it comes to certification, or questions on whether technical components were available but seemed, for instance in the security questionnaire, not broad enough. The first remark needs to be shifted to the certification part, in which the CRISP Methodology, its relation to the requirements of the S-T-E-Fi dimensions and the requirements for certification are explained (see chapter 3.2.1 of this report). However, it is to highlight, that the evaluation part is not synonymous with the certification part as illustrated also in Figure 20 on page 41. With its multidimensional approach, the CRISP project addresses the gap in current certification landscape by including social / human factors in the evaluation of security PSS, which is stated for instance by the European Commission. To seize the suggestion for the second remark from workshop participants, information on technical components of a security solution will be requested from a ‘project leader’ and included into the first Evaluation Report (R1), serving as information source for the assessors (‘project participants’). Confidentiality will be required then.

The definitions of the S-T-E-Fi dimensions as to each criterion presented during the assessment exercise were not incorporated in the online questionnaire. These definitions will be added once the implementation of the CRISP evaluation part is clearly determined.

A practical issue and also interesting to know was how long approximately it would take the ‘project participants’ to answer the questionnaires. With the exception of the Fi questionnaire, the participants needed between 15 and 20 minutes on average to respond to the questions. Especially the participants in the international workshops working with the Fi questionnaire needed the longest time for their answers (up to almost 40 minutes). This specification is not representative or should be overstated, however it shows that Fi associated attribute questions seem to be more challenging for the participants. This may have different reasons underlying in the testing situation, such as the larger number of associated attribute questions (in comparison to those of the other dimensions). This observation will be dealt with properly when updating the evaluation criteria list in the upcoming project work.

---

32 Kamara, et al., op cit., June 2015.

5. **Online questionnaire handling:**

As the evaluation criteria questionnaire was transformed into an online format, some issues raised, such as the ‘possibility to turn back pages’ and, in this matter the ‘possibility to change answers’.

**To be learned from the workshops:**

This remark is just a technicality and can be solved easily for the online version of the evaluation criteria questionnaire by including a “back” button which allows skipping back to pages. This issue is not existent in case the assessment will be performed by using a ‘paper and pencil’ questionnaire format.

6. **Others: More than one stakeholder in the same dimension**

**To be learned from the workshops:**

Using the international workshop on Alarm Systems/CCTV as an example, three stakeholders were allocated to the S dimension, two participants to the T dimension and two to the Fi dimension (see Table 3 on page 28 of this report). A first analysis of the questionnaire output shows that the “consultation” box in the questionnaire was most frequently ticked (see Figure 18). This goes in line with the feedback that more information on the scenario was necessary.

To address the issue of subjectivity of ‘project participants’ as assessors for a security PSS, the exercise findings in the context of the Alarm Systems/CCTV Workshop show, that only for the Fi dimension, the yes/no response regarding “Is there any other less privacy intrusive alternative?” (Criterion “privacy”) and “Does the security solution require that the controller has technical and organisational measures for the security of personal data?” (Criterion “personal data”) differed between stakeholders, as one Fi expert answered the question with ‘yes’ and the other with ‘no’. Similar incidents were observed in the context of the Drones Workshop output regarding the T dimension. Adding space for an additional answer to all associated attribute questions\(^{34}\) will allow to express the respective decision and will also externalise why the answer was given (yes/no and qualitative responses are to be included in the Overall Evaluation Report R\(_2\) and, in case of deviations, forwarded to a ‘project participant’ and an external auditor who will receive the Evaluation Report and decide, far from subjectivity, upon the worthiness of the security PSS for a certificate based on requirements for certification).

As introduced in Table 7 “Stakeholder groups and intended allocation to S-T-E-Fi dimensions” presented in CRISP report 5.1\(^{35}\) and explained again in chapter 2.1.2 of this report, the allocation of stakeholders to the S-T-E-Fi dimensions is based on their

\(^{34}\) As foreseen in the four level structure of the S-T-E-Fi approach (see also Figure 14).

\(^{35}\) Hempel, et al., op. cit., October 2015, p. 49f.
respective expertise. In reference to an assumption of a workshop participant, it is indeed possible that one stakeholder can be assigned to all S-T-F-Fi criteria (e.g. politicians). This, however, is not a general rule or requirement which, for instance, becomes apparent from the Fi dimension that requires data protection knowledge. To cover all potential eventualities, the stakeholders in the second national workshop were allocated to all four dimensions for testing purposes. The results are still pending. However, at this point there is no motivation to revise Table 7 “Stakeholder groups and intended allocation to S-T-E-Fi dimensions” presented in CRISP report 5.1.

Figure 18: response rate of the alarm systems/CCTV workshop participants
Note: ‘Questions fulfilled’: response in the majority was clearly ‘yes’; ‘Questions not fulfilled’: response in the majority was clearly ‘no’.

36 See Hempel, et al., op. cit., October 2015, p. 49.
2.4 Main conclusions for the evaluation part of the CRISP methodology and resulting recommendations

The discussions with the external stakeholders during all scenario-based workshops were very focused, targeted, and helpful for a further refinement. Based on the feedback provided, the main conclusions can be summarised as follows and will be expressed as recommendations for further research work:

It is important to demonstrate, that CRISP evaluation is the first stage belonging to the overall methodology, followed by certification. The first Evaluation Report (R₁) needs to summarise the main information including the technical components, which serves as the input for the assessment stage and as an information source for ‘project participants’ as assessors. The two-stage questioning as part of the evaluation criteria questionnaire (yes/no questions, followed by a qualitative question) allows to specify the assessment and possibly will reveal individual perceptions towards a security PSS. The second Evaluation Report (R₂) will serve as the basis for certification and present the overall findings of the security PSS assessment including a listing of potential conflicts and deviations within and between S-T-E-Fi criteria that is presented to the ‘project leader’ and an external auditor. Finally, it is an auditor and not ‘project participants’ as assessors themselves who will carry out the third-party attestation and thus relate potential conflicts to standards and existing regulations.

Based on the outcome of the workshops, the proposed Overall Evaluation Report (R₂) is now slightly modified, as presented in Table 4.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• configuration stage output confidential R₁ which includes technical components necessary for the assessment of a security PSS</td>
<td>• configuration stage output confidential R₁ including technical components plus further information, such as uploaded (confidential) information, evidence, stakeholder participation</td>
</tr>
<tr>
<td>• personal contributions per actor role during the assessment stage</td>
<td>• general reflexivity description (how many assessment questions were answered, not answered, fulfilled, not fulfilled, consultations etc.)</td>
</tr>
<tr>
<td>• if applicable, assessment analysis of potential conflicts within the same S-T-E-Fi criteria.</td>
<td>• listing and description of potential conflicts within and between S-T-E-Fi criteria</td>
</tr>
</tbody>
</table>

Although the evaluation part works as an input, the main conclusions and recommendations for the certification part as presented in chapter 3.3 of this report, foremost the specification of the scope of the certification scheme and its requirements, will influence the evaluation part as well.
Hence, some of the recommendations to elaborate on or discuss in the context of the evaluation part come together with those for the certification part.

<table>
<thead>
<tr>
<th>recommendation</th>
<th>what will be done</th>
<th>When</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Identifying the terms (not to be mixed up with criteria) that are not self-explanatory or ambiguous in the evaluation criteria questionnaire as well as provide a clearer language of the assessment questions. Based on the scope of the certification scheme (see the decision of the scope in chapter 3.3.1 of this report), the evaluation criteria from CRISP report 4.3 will be revised and discussed within WP 6. The associated attribute questions (yes/no-question answers) will be revised in this context as well (number of associated attribute questions per criterion, language of the questions, wording used). Terms that are not self-explanatory or ambiguous will be defined within the evaluation criteria questionnaire or in a separate document additionally. It is aimed at avoiding ‘interpretability of questions’.</td>
<td>WP 6</td>
</tr>
<tr>
<td>2</td>
<td>Thinking carefully about the implementation of the CRISP evaluation part. Here, attention should be given to the institution that will carry out the evaluation part or is going to be the first contact. This recommendation will be worked out in detail in the upcoming project work of WP 6 and documented accordingly.</td>
<td>WP 6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WP 7</td>
</tr>
<tr>
<td>3</td>
<td>Harmonising the two evaluation stages (configuration and assessment) and their outputs. This recommendation will be paid closer attention to during CRISP research work of WP 6 and will also addresses the quantitative/qualitative question formats, as well as all conflict relations between and within S-T-E-Fi dimensions. The questionnaire results gained from the scenario-based workshops will serve as further input in particular for the proposed Evaluation Reports (R1 and R2).</td>
<td>WP 6</td>
</tr>
<tr>
<td>4</td>
<td>Deciding how the criteria definitions based on the explanation presented in CRISP report 4.3 can be implemented in the evaluation criterion questionnaire. This depends on the outcome of No. 4.</td>
<td>WP 6</td>
</tr>
</tbody>
</table>
3 CERTIFICATION PART OF THE CRISP METHODOLOGY

As already explained in chapter 1.1 of this report, the international workshops were mostly focused on debating about the outcome of the certification part, as experts on certification and standardisation were invited for this purpose. Nevertheless, feedback provided by national workshop attendees are included in the following explanations.

3.1 GENERAL PREPARATION APPROACH FOR THE WORKSHOPS

During the preparation for the workshops, based on the recommendations from the Validation Workshop\textsuperscript{37}, a closer look has been taken on the main elements of the certification scheme based on the ISO/IEC 17067:2013.\textsuperscript{38}

The CRISP consortium partners provided information on the main elements as described in chapter 6.5.1 of ISO/IEC 17067:2013 based on the information sources investigated for the previous work packages (WPs). This information was discussed within the CRISP consortium during a number of GoToMeetings. The preparation process can be schematically shown as follows:

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure19.png}
\caption{preparation process for the discussion of the certification part of the CRISP Methodology during the international scenario-based workshops}
\label{fig:preparation_process}
\end{figure}

\begin{itemize}
\item \textbf{Collection}: Aligning main elements of the certification scheme (chapter 6.5.1 of ISO/IEC 17065) with WP 5, WP 6 and WP 7.
\item \textbf{Discussion}: Discussing the context of each main element of the certification scheme belonging to WP 5.
\item \textbf{Selection}: Determining which of the main elements can be based on the general requirements to the certification scheme and which of them require a formulation specifically for CRISP.
\item \textbf{Conclusion}: Summarising the context of the requirements specifically necessary for the CRISP certification to be discussed during the scenario-based workshops.
\end{itemize}

\textsuperscript{37} See Hempel, et al., op cit., October 2015.

\textsuperscript{38} A certification scheme describes “rules, procedures and management for carrying out certification related to specified products, to which the same specified requirements, specific rules and procedures apply” (ISO/IEC 17065:2012 'Conformity assessment - Requirements for bodies certifying products, processes and services').
As shown in Figure 19, the preparation process consisted of four main steps: collection, discussion, selection and conclusion. Each of these steps had one or two tasks.

The chosen main elements of certification scheme with their specific issues are depicted in Table 4.

The information provided in Table 5 was used during the international scenario-based workshops as a basis for the discussion of the main elements of the CRISP Certification Scheme. In the following chapter, the debate on these main elements and their specific requirements and issues are described per main element each.

### Table 5: the proposed context of the selected elements of the certification scheme

<table>
<thead>
<tr>
<th>No.</th>
<th>main elements of a certification scheme</th>
<th>the specific issues for CRISP to be discussed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The <strong>scope</strong>, including the type of products covered</td>
<td>Three possible ways to narrow the scope: 1. Group security PSS based on the 12 functions (proposed taxonomy). 2. Narrow the scope of PSS based on the engagement of all 4 S-T-E-Fi dimensions. 3. Choose two/three application areas, for instance drones, CCTV and alarm systems, and propose a certification scheme for these areas with a possible extension to other application areas.</td>
</tr>
<tr>
<td>2</td>
<td>Other <em>(specific) requirements</em> to be met by the client</td>
<td>Three specific requirements: 1. Pass the evaluation part of the CRISP Methodology. 2. Early involvement of stakeholders in the evaluation part of the CRISP Methodology. 3. Fulfilment of requirements of a Quality Management System.</td>
</tr>
<tr>
<td>3</td>
<td>The <strong>requirements for certification bodies</strong> and other conformity assessment bodies involved in the certification process</td>
<td>Two specific requirements: 1. Assessment by the trained scientists in case of certification of the new technology (for example drones). 2. List of organisations specialised on S-T-E-Fi dimensions.</td>
</tr>
<tr>
<td>4</td>
<td>The <strong>information to be supplied</strong> for the certification body by an applicant for certification</td>
<td>One specific information and one condition: 1. Combination of the Overall Evaluation Report with all technical support documentation. In case of the second assessment: a list of actions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to solve the conflicts and what has been done</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>------------------------------------------------</td>
</tr>
</tbody>
</table>
| 5 | How **non-conformities** with the certification requirements are to be dealt with and resolved | Issues to be discussed:  
1. Identification of minor non-conformities based on the relevance of the requirements per dimension.  
2. Possibility for corrective actions based on the evaluation report in case of minor non-conformities.  
3. Extent to which the requirements on the S-T-E-Fi dimensions have to be fulfilled per dimension (proposal: S 100%, T min 70%, E min 70%, Fi 100%).  
4. An acceptable number of conflicts. |
| 6 | General **conditions for granting, maintaining, continuing, extending, reducing the scope of**, suspending and withdrawing certification | Issues to be discussed:  
1. Timeframe for the CRISP certification process: 6 months in total, 3 months max for the evaluation part including pending (corrective actions) and 3 months max for the certification part including pending (corrective actions).  
2. Timeframe of validity of CRISP certificate: 3 years. |

Source: @Haponava, January 2016.
3.2 THE DEBATE ON THE CHOSEN MAIN ELEMENTS OF THE CERTIFICATION SCHEME

3.2.1 Introduction to CRISP’s Methodology, its relation to the requirements of the S-T-E-Fi dimensions and the requirements for certification

For a better understanding of the CRISP Methodology and its relation to the evaluation criteria and requirements for certification, Figure 20 was introduced and explained during the international workshops.

**Figure 20: CRISP Methodology and its relation to the evaluation criteria and requirements for certification**

Source: @Haponava, January 2016.
As already described in CRISP report 5.1 and shown in Figure 1 (p. 9), the CRISP Methodology consists of two parts, the evaluation part and the certification part.

**Evaluation part**

During the evaluation part, an assessment of security PSS is to be carried out, according to the requirements based on the evaluation criteria as defined and described in CRISP report 4.3\textsuperscript{39}. Some of the evaluation criteria have been identified based on the current European normative documents, such as legislation and European standards. Other evaluation criteria have been chosen on the basis of relevant literature sources and research project outcomes. All identified evaluation criteria will be used to formulate the requirements in a common normative document. This document will be a result of the CEN Workshop Agreement (CWA), which belongs to CRISP’s Task 7.5 of WP 7 and thus offers the opportunity to use the CWA as the foundation of further standardisation activities, developing a European standard within the next years.

**Certification Part**

Granting a CRISP Certificate is based on the requirements for CRISP certification. These requirements are a combination of general requirements used in certification and the requirements specifically developed for the CRISP project. For the general requirements, references will be drawn from the well-known ISO/IEC standards, while the requirements that are specific for the CRISP project will be defined based on the conclusions and recommendations from the scenario-based workshops. Both the general and the specific requirements will be covered by the CRISP Certification Scheme.

After introducing an explanation of the overall Figure 1 (p. 9), the experts had a clear idea of the CRISP Methodology and did not have any remaining questions.

### 3.2.2 Debate on the chosen main elements of the certification scheme and their specific issues

In this section, the general discussion on the proposed context of the elements of CRISP certification scheme will be described per element with the comparison of the results and the main conclusions made by the CRISP consortium afterwards.

#### 3.2.2.1 The scope of the certification scheme

The discussion on the scope of the CRISP certification scheme started with the question how to narrow the scope down. Three options have been proposed for discussion:

\textsuperscript{39} Kamara, et al., op cit., June 2015.
1. **Group the PSS according to the 12 functions presented in CRISP’s taxonomy (as proposed in CRISP report 1.2)**

The discussion started with highlighting the difference in functions between security products, systems and services. Both, the experts on Drones and the experts on intelligent CCTV-systems agreed that the functions of the products are well covered by technical specifications described in the European standards. Systems, on the other hand, besides various components with different functions have also got installation which can be modified by the installers. According to the experts on Drones, it is not easy to certify installations as installations can be easily modified. In contrary, the experts on CCTV believed that a certification scheme for security systems will be a great contribution to the security industry and should be seen as a set of the aligned security products and services.

The experts on Drones believed that services are difficult to certify due to:

- the variety of possible functions to be performed by the service providers and
- the lack of the standards in this specific application area.

However, according to them, the services are the most important to be assessed and approved in the case of drone certification. The experts proposed to certify the provider of the service rather than the service itself.

The experts on CCTV believed that it won’t be difficult to certify services on CCTV because this topic is partly covered by the existing standards. Here, the experts named services as an important aspect and mentioned some variety in the type of services. For example, the access of personal monitoring data, the guarding on the ground and the alarm system maintenance are different types of services, which could be covered by the CRISP certification with a reference to already existing standards.

During the discussion, the experts on CCTV highlighted several times the importance of certifying only security systems, which include products and services as components. According to them, choosing security systems as a scope will bring together the existing certification of the security products and the use of existing standards for security services. They also highlighted that certification of security systems will allow assessing all components of a system as a whole and not individually. This will cover the gap in certification, which exist on the European market of the security PSS.

In general, the experts did not see how the grouping based on the functions could reduce the scope for the CRISP certification scheme. Both, the experts on Drones and on CCTV were unanimous that the function-oriented approach will not work that well. They also mentioned that the proposed taxonomy does not foresee the unintended functions which could lead to many problems while certifying the security PSS.

---

2. **Narrow the scope of PSS based on the engagement of all S-T-E-Fi dimensions to be used as a condition**

According to the experts, this option would be difficult for certification as it might be applicable only to some products and services and would be related to the issues that the certification does not address. Besides, security PSS cover very different aspects of the S-T-E-Fi dimensions. The experts believed that taking into account all four dimensions would lead to a tremendous amount of S-T-E-FI assessments for each PSS. However, during the Evaluation part of the CRISP Methodology the engagement of all four S-T-E-Fi dimensions can be used as a condition for certification. In other words, the security PSS should cover all four S-T-E-Fi dimensions. Here, the experts on CCTV highlighted again the importance of choosing security systems for CRISP certification. Moreover, the experts stated that the $S$ dimension is well covered by the existing European standards. They advised to refer to the standards while evaluating the $S$ dimension and to focus on the other three dimensions.

3. **Choose one/two/three application areas, for example drones, CCTV and alarm systems, and propose a certification scheme for these areas with a possible extension to other application areas**

Both experts on Drones and CCTV agreed that this option is the most visible one and proposed to choose alarm systems as an application area where CCTV is part of it. The reasons for their choice were named as follows:

<table>
<thead>
<tr>
<th>Aspect</th>
<th>DRONES</th>
<th>ALARM SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maturity</td>
<td>Drones are a too ambitious and too undeveloped area.</td>
<td>Alarm systems is a more developed area, which means that is it more bounded and specific.</td>
</tr>
<tr>
<td>Existing certification</td>
<td>Certification on drones will lead to certification of services, both private and public.</td>
<td>There is certification of the security products that can only enhance the CRISP certification of the security system.</td>
</tr>
<tr>
<td>Existing standards</td>
<td>There are no developed and recognised European EU standards to be used as a basis for the certification.</td>
<td>There are a lot of EU standards in the area of alarm systems available.</td>
</tr>
</tbody>
</table>

Source: @Haponava, January 2016.
During the discussion of the scope for the CRISP certification the experts have made some recommendations that can be summarised as follows:

- to use the existing European standards to evaluate the **S** dimension and to focus on social and ethical aspects, in other words, the **T**, the **E** and the **Fi** dimensions while assessing the fulfilment of the S-T-E-Fi requirements;
- to consider unintended use and function. This might be an endless task, but according to the experts, some unintended uses are well known already;
- to think carefully about the implementation of the CRISP certification scheme as this is the key;
- to define the owner of the certificate; and
- to provide a matrix with ISO standards to be used for the CRISP certification scheme.

The last three recommendations will be addressed in CRISP’s WP 6.

### Reaction of the CRISP consortium and the final choice for the scope of the CRISP certification:

Based on the strong recommendations of the experts on CCTV, the CRISP consortium decided to choose security systems as the scope of the CRISP certification. As stated earlier, the security systems include security products and services as components.

Besides, the CRISP consortium decided to narrow the scope for the CRISP certification by choosing Alarm systems as an application area. The consortium proposed to adapt the scope of Alarm systems from CLC/TC 79 “Alarm systems”\(^\text{41}\), which includes the following systems:

- intruder and hold-up alarm systems
- access control systems
- periphery protection systems
- combined alarm-fire alarm systems
- social alarm systems
- CCTV-systems
- other monitoring and surveillance systems related to security applications as well as
  - associated and dedicated transmission and communication systems.

The scope adapted from CLC/TC 79 will help in the future to align the results of the CRISP project to the European standardisation activities.

---

3.2.2.2 Other (specific) requirements to be met by clients

Three specific requirements were proposed for the discussion during the workshops:

1. Pass the evaluation part of the CRISP Methodology
2. Early involvement of stakeholders in the evaluation part of the CRISP Methodology
3. Fulfilment of requirements of the Quality Management System

The discussion of these proposed specific requirements was quite limited as the experts found them reasonable and agreed on them.

The first specific requirement should be fulfilled as evaluation based on the S-T-E-Fi dimensions is a part of the whole CRISP Methodology.

The second requirement is needed to be able to evaluate security PSS from the different stakeholder perspectives and, hence, to receive a total picture of the PSS. For the second requirement on the early involvement of stakeholders, the experts proposed to require the names of the stakeholders involved in the Evaluation part and their organisations in order to check their competence in evaluating the security PSS.

Fulfilment of requirements of the Quality Management System as the third requirement was accepted by experts as they believed that quality is an essential part of any PSS and has direct relation to the security services.

3.2.2.3 (Specific) requirements for certification bodies

Two requirements were discussed for this element:

1. The certification of the new technologies for example Drones, certification was proposed to be done by trained scientists;
2. Availability of the list of organisations specialised in certification of S-T-E-Fi dimensions.

In regard to the trained scientists, all experts agreed that certification should be done by trained experts, and not scientists. However, they suggested the involvement of scientists in the evaluation part of the CRISP Methodology.

Concerning the list of organisations specialised in S-T-E-Fi dimensions, the experts did not see this requirement as a special one for certification bodies as this is the standard task of accreditation bodies. Here, the experts noticed that certification bodies have to be accredited by a recognised accreditation body. The accredited certification bodies provide the applicants with certainty of their neutrality, independence and competence. This statement is in line with the recommendation given during the Validation Workshop earlier in the CRISP project (CRISP report 5.1, p. 34).
3.2.2.4 The information to be supplied for the certification body by an applicant for certification

For this element only one specific information set was identified, which is a combination of the Overall Evaluation Report (R2)\(^{42}\) with all technical support information.

As the CRISP Methodology gives an opportunity to go several times through the evaluation part, in case of a second assessment, a list of actions which needs to be done to solve the identified conflicts, is required as well.

The experts agreed on these requirements for information to be supplied. In addition, they proposed to ask for provision of “good practices” or code of conduct while assessing services.

**Reaction of the CRISP consortium:**

The CRISP consortium found useful the recommendation of adoption of a code of conduct for the participants of the scheme and/or a guidance document on “good practices”. This will be considered in a more mature stage of the project, after the finalisation of the basic elements of the CRISP scheme and the feedback from the stakeholders in WP6 (certification bodies, data protection authorities, etc.).

3.2.2.5 Non-conformities with certification requirements

The discussion of non-conformities was narrowed down by four issues:

1. *Identification of minor non-conformities based on the relevance of the requirements per S-T-E-Fi dimension*

The experts confirmed that the identification of the minor non-conformities will depend on the requirements of S-T-E-Fi dimensions and their relevance. They discouraged to use the weightings while ranking the requirements in order to emphasize the importance of some requirements within each dimension. They believed that the weightings might be very subjective and too complex. Their suggestion was to think about some general criteria based on which a distinction could be made in the importance of the requirements.

**Reaction of the CRISP consortium:**

The CRISP consortium seriously examined this suggestion and came up with a proposal to use the alignment with the existing legislation, if applicable existing regulations, and the European (EN) standards as a main indicator while identifying the relevance of the S-T-E-Fi requirements. This indicator will allow defining the minor and major non-conformities.

---

2. **Possibility for corrective actions based on the evaluation report in case of minor non-conformities**

The experts agreed on giving an opportunity for corrective actions of minor non-conformities based on the reports from the evaluation part of the CRISP Methodology.

3. **Extent to which the requirements on the S-T-E-Fi dimensions are fulfilled per dimension**

While discussing this issue, a gradation of the S-T-E-Fi dimensions was proposed to be used to identify the extent to which the requirements on the S-T-E-Fi dimensions are fulfilled per dimension. This gradation was proposed to express in percentages (%). For example, the S- and the Fi dimensions were estimated by the CRISP consortium as very important and therefore all requirements of these two dimensions should be fulfilled for 100%. On the other hand, the T and the E dimensions were seen as less important in comparison with the S and Fi dimensions. The consortium assumed that the fulfilment of 70-80% of the requirements of the T and the E dimensions would be enough to move further to the Certification part. This proposed gradation was discussed during the workshops.

Both, the experts on Drones and on CCTV agreed that gradation expressed in percentages is not the best choice to go with. While the experts on Drones proposed to use a “pass/no pass” approach and were less enthusiastic in using gradation for certification, the experts on CCTV were keen on gradation and suggested to use for these purposes points rather than percentages.

The experts on CCTV believed that gradation in certification will lead to more competitive market. They also highlighted that the gradation of the S-T-E-Fi dimensions will much depend on the situation where security systems are used. According to them, a difference should be made between high, medium and low security systems, where one dimension would be more important to be fully fulfilled than the other one. In their example, a high security system should fulfil all requirements on the S dimension but not necessarily all requirements on the Fi dimension depending on the primary goal of the system.

The strong link between the requirements on the S-T-E-Fi dimensions and the situation where security PSS are used is a confirmation of one of recommendations made earlier in the CRISP project during the Validation Workshop. There, the experts recommended taking into account the context in which the security PSS is used as a part of the certification process and using standards and certification contextually (see CRISP report 5.1, p. 34).

During the discussion on the extent to which the requirements on the S-T-E-Fi dimensions have to be fulfilled, the experts raised a question regarding the fulfilment requirements of the T and Fi dimension. They believed that the most requirements are hard to evaluate based on their qualitative nature and proposed to assess the efforts made in order to fulfil the qualitative requirements.
4. An acceptable number of conflicts (based on the summary of the Evaluation R3)

This issue did not receive a required attention during the workshops but was discussed during a CRISP consortium meeting after the scenario-based workshops.

**Reaction of the CRISP consortium:**

As a result of this discussion, the CRISP consortium partners concluded that an acceptable number of conflicts depends on the conflicts, the main purpose of using security PSS and the situation/scenario where they are used. This is up to an auditor to estimate whether the identified conflicts are acceptable to grant a certificate.

3.2.2.6 General conditions for granting, maintaining, continuing and extending the scope of certification

In this topic only two issues have been discussed which were:

1. An overall timeframe of the Evaluation and Certification based on the CRISP Methodology

In regard to the first issue, the proposal from the CRISP consortium was to limit the timeframe to six months in total, where maximum three months are given for passing through the evaluation part including time for corrective actions, if needed. The remaining three months, including time for corrective actions as well, aim at passing through the certification part of the CRISP Methodology. The proposal of the CRISP consortium on the overall timeframe can be visualised as follows:

![Diagram](image)

**Figure 21: the proposal of the CRISP consortium on the overall timeframe**

Source: @Haponava, January 2016.
In general, the experts on Drones agreed on the proposed timeframe and suggested to make differentiation in existing technologies and new technologies. According to them, new technologies should have more flexibility in time.

On the other hand, the experts on CCTV highlighted that time should be indicated based on the time spent on the evaluation and certification parts of the CRISP Methodology rather than on the fixed period of time for the whole evaluation and certification process. They suggested to use an implementation plan for CRISP’s evaluation and certification, where application for a CRISP certificate is limited by one year.

2. **Time of validity of the CRISP certification scheme**

The proposal of the CRISP consortium to use three years as a validity period of the CRISP certification certificate was accepted by the experts with a remark of one condition: There should be no changes in the assessed security PSS and their situation/scenario they are used.

### 3.3 Summarising the main conclusions and recommendations for the certification part of the CRISP Methodology

#### 3.3.1 Main conclusions

Based on the discussion of the main elements of the CRISP certification scheme during the Validation and scenario-based workshops and the recommendations from the experts, the main conclusions on the certification part of the CRISP Methodology can be summarised as follows:

<table>
<thead>
<tr>
<th><strong>Scope</strong></th>
</tr>
</thead>
</table>
| The CRISP Certification Scheme will focus on the security systems, which includes in particular: intruder and hold-up alarm systems, access control systems, periphery protection systems, combined alarm-fire alarm systems, social alarm systems, CCTV-systems, other monitoring and surveillance systems related to security applications as well as associated and dedicated transmission and communication systems. The security services such as access of personal monitoring data, the guarding on the ground and the alarm system maintenance will be a part of the security systems.  
The classification of the security PSS according to the 12 functions presented in CRISP’s taxonomy was not seen by experts as visible and therefore will not be taken on further in this project.  
The fulfilment of requirements on S-T-E-Fi dimensions will be used as a condition with the focus on social and ethical aspects |

<table>
<thead>
<tr>
<th><strong>Other (specific) requirements to be met by clients</strong></th>
</tr>
</thead>
</table>
| The applicant will be asked to fulfil the following specific requirements:  
| **a.** Pass the evaluation part of the CRISP Methodology  
| **b.** Early involvement of stakeholders in the Evaluation part of the CRISP Methodology, |
where the stakeholders have to provide their names and their organisation in order to check their competence in evaluating the security system

c. Fulfilment of requirements of Quality Management System.

(Specific) requirements for certification bodies
Certification bodies shall be accredited on the basis of the requirements in ISO/IEC 17065. No specific requirements for certification bodies will be used in the CRISP Certification Scheme.

The information to be supplied to the certification body by an applicant for certification
An applicant will be asked to provide a combination of the Overall Evaluation Report with all technical support information.
In case of the second assessment, a list of actions done to solve the identified conflicts is required as well.

Non-conformities with the certification requirements
Non-conformities will be determined based on the alignment of the requirements on the S-T-E-Fi dimensions with the existing legislation and the European (EN) standards.
A possibility for corrective actions of minor non-conformities based on the Overall Evaluation Report will be given.
An extent to which the requirements on the S-T-E-Fi dimensions are fulfilled per dimension should be individually assessed by an auditor based on the situation/scenario where security systems are used.
The fulfilment of the requirements on the T and E dimensions will be assessed based on the efforts done by an applicant to fulfil them.
Assessment of the identified conflicts depends on the nature of conflicts and will be done based on the main purpose of using security system and the situation/scenario where it is used. This is up to an auditor to estimate whether the identified conflicts are acceptable to grant a certificate.

General conditions for granting, maintaining, continuing, extending the scope of certification
The time for the whole Evaluation and Certification process based on the CRISP Methodology should not exceed one year.
The CRISP certificate is granted for a maximum period of three years. During the term of validity, the certification body shall verify that the certified security system still fulfils certification requirements.
The certificate holder will be obliged to report promptly any expected changes in the
security system before putting the modified system on the market as certified according to the CRISP Certification Scheme.

### 3.3.2 Main recommendations

A summary of the main recommendation given by the experts during the scenario-based workshops is shown in Table 7.

#### Table 7: the main recommendations on the discussed elements for CRISP certification

<table>
<thead>
<tr>
<th>No</th>
<th>Recommendation</th>
<th>What will be done</th>
<th>When</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>To use the existing European standards to evaluate the S dimension and to focus on the social and ethical aspects, in other words, the T, the E and the F dimensions while assessing a security system.</td>
<td>The evaluation criteria from CRISP report 4.3(^{43}) will be revised and discussed within WP 6. The revised criteria will be used in task 7.5 of CRISP’s WP 7 to formulate the requirements for the security systems with the focus on the social and ethical aspects.</td>
<td>WP 6  WP 7</td>
</tr>
<tr>
<td>2</td>
<td>To consider some well-known unintended uses and functions.</td>
<td>This recommendation will be further discussed during the round table with the certification bodies.</td>
<td>WP 6</td>
</tr>
<tr>
<td>3</td>
<td>To think carefully about the implementation of the CRISP certification scheme. Here, attention should be given to the estimated costs for the CRISP certificate. The recommendation is that the costs should not be higher than 5 percent of total costs of the security system.</td>
<td>This recommendation will be worked out in detail and documented in CRISP report 6.1 and CRISP report 7.4.</td>
<td>WP 6  WP 7</td>
</tr>
<tr>
<td>4</td>
<td>To define the owner of the certification scheme.</td>
<td>This recommendation will be worked out in detail in DEL 6.1.</td>
<td>WP 6</td>
</tr>
<tr>
<td>5</td>
<td>To provide a matrix with ISO standards to be used for the CRISP certification.</td>
<td>This recommendation will be a part of the final Certification Manual, DEL 6.2</td>
<td>WP 6</td>
</tr>
<tr>
<td>6</td>
<td>To ask for provision of “good practices” or code of conduct while assessing security services.</td>
<td>This recommendation will be considered while developing a roadmap and will be added to the list of final</td>
<td>WP6, WP 7</td>
</tr>
</tbody>
</table>

---

\(^{43}\) Kamara, et al., op cit., June 2015.
<table>
<thead>
<tr>
<th>No</th>
<th>Recommendation</th>
<th>What will be done</th>
<th>When</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To differentiate between high, medium and low security systems, hence to consider the context of use as a part of the certification process.</td>
<td>This recommendation will be added to the list of final recommendations at the end of the CRISP project.</td>
<td>WP 7</td>
</tr>
<tr>
<td>8</td>
<td>To require an implementation plan for CRISP Evaluation and Certification, where application process for a CRISP certificate is limited by 1 year</td>
<td>This recommendation will be further discussed during the round table with the Certification Bodies, task 6.3.</td>
<td>WP 6</td>
</tr>
</tbody>
</table>
4 CONCLUSION BASED ON THE WORKSHOP OUTCOMES

The feedback provided by all stakeholders regarding the CRISP Methodology in the context of the workshops was reflected on by the CRISP consortium afterwards. In order to foster greater acceptance and usability, specific parts of the CRISP Methodology were edited accordingly in conclusion to the experts’ feedback and recommendations wherever appropriate for the overall purpose of the CRISP project.

Finally, this report concludes with the refinements to be carried out on the CRISP Methodology by depicting the development of the CRISP Methodology from its very beginning until up to now.

Figure 22 presents the first draft version of the CRISP Methodology, which was used as initial point to incorporate the S-T-E-Fi conflict review as a part of evaluation and certification. This first draft was presented and explained during the Validation Workshop on September the 3rd, 2015. The initial idea (flowing crossovers between CRISP’s evaluation and certification part, in which evaluation will lead to certification) was not supported by the experts on standardisation and certification.

Figure 22: draft version of the CRISP procedure presented at the Validation Workshop (September 2015)
Source: @Hirschmann 2015.

The CRISP consortium thus executed the expert’s opinion in concluding with a stronger separation of both parts: starting with the evaluation of a security PSS using application scenarios fist, followed by the certification part. At this point, it was already clear that the evaluation part itself does not lead to certification.\[^{44}\] This is illustrated in Figure 23. The

\[^{44}\] See Hempel, et al., op cit., October 2015, p. 48.
result of the modification, as pictured in Figure 23, was presented in CRISP report 5.1.45 The modification of the first draft also referred to the graphical presentation of ‘Report 1’ and ‘Report 2’: It was changed according to the more conventional presentation in certification landscape: R₁, R₂, R₃ are the outputs of one activity (configuration, assessment, and audit), which work as the input for another activity (assessment, audit, and attestation).

![Diagram](image.png)

**Figure 23: first refinement resulting in CRISP’s Evaluation and Certification Methodology as presented in CRISP report 5.1 (October 2015)**


Based on the outcome of the debates at the scenario-based workshops, the proposed certification part of the CRISP Methodology, as shown in Figure 24, is, again, slightly modified.

The following changes were performed:

1. **The conformity assessment function of “inspection”, or, in other words, on-site assessment, was added to the function of “auditing”**

During the feedback discussions, it became obvious that just to assess the provided documentation will not be enough to attest a security system and should be extended in the on-site assessment. This on-site assessment is necessary to verify that some statements from the Overall Evaluation Report conform to the requirements of the CRISP certification. Based on the ISO/IEC 17000:2014, this function is performed by inspection, defined as “examination of a product design, product, process or installation and determination of its conformity with specific requirements or on the basis of professional judgment, with general requirements”.

---

45 Hempel, et al., op cit., October 2015, p. 42.
2. *The conformity assessment function of “surveillance” was added*

In chapter 6.2.1 of CRISP report 5.1, the decision to exclude surveillance as a standard function as it is not always performed within the certification process was made. However, the results of the scenario-based workshops highlighted the need for surveillance in order to control any changes in a security system and to maintain the validity of the CRISP Certificate.

Therefore, it was decided to add the function “surveillance” to the certification part of the CRISP Methodology. The visualisation of the actual CRISP Methodology is shown below.

![Figure 24: the modified and current CRISP Methodology.](image)

Source: @Haponava, January 2016.

In conclusion, the scenario-based workshops allowed an active exchange between practitioners and researchers and contributed to a further validation of the CRISP Methodology presented in the first deliverable report of WP 5. All workshop activities aimed at ensuring a strong stakeholder involvement and feedback towards the developed methodology from both the supply and demand side of security PSS, as well as other relevant stakeholders. The stakeholder’s feedback and their recommendations were reflected by the CRISP consortium and the methodology, particularly the certification part, was edited and amended accordingly. Hence, the modified CRISP Methodology, the main conclusions and recommendations from chapter 2 and 3 of this report will need to be included in the forthcoming work in order to develop a clear roadmap and certification manual (as part of CRISP’s WP 6) and, finally, enhance acceptance of the proposed certification scheme (as part of CRISP’s WP 7).

Last but not least, the CRISP consortium wants to thank all workshop attendees for their great interest in the project activities and their active participation during all validation activities.
LIST OF REFERENCES


Hopf, Christel, “Forschungsethik und qualitative Forschung“, in Uwe Flick, Ernst von Kardorff, and Ines Steinke (Hg.), Qualitative Forschung. Ein Handbuch. Reinbek bei Hamburg, Rowohlt Taschenbuch Verlag, pp. 589-600.


