Study of support for the design and secure interoperability of multiple IoT applications

Version
Version 1.1

Lead Partner
EC - JRC

Date
13/04/2017

Project Name
ARMOUR – Large-Scale Experiments of IoT Security Trust
Abstract

D4.2 investigates how different security and privacy solutions and products can be used in a harmonised way to support the design and deployment of secure IoT applications. In the IoT domain, this goal is more challenging than other domains because of the presence of many different heterogenous technologies and applications, which are usually implemented in a vertical manner due to market forces, boundary conditions and operational constraints. The deliverable describes three key elements for achieving this goal: the first element is to analyze the strengths and weaknesses of security certification in the IoT domain. Security certification has a long history from its origins in the defense domain (e.g., Orange Book), but its application in the IoT domain can present challenges, which are identified and described. Then, a potential certification framework to address these challenges is presented. The framework is based on the concepts presented in the other deliverables of ARMOUR. The second element is to define a design, which takes in consideration the dynamicity of IoT and the definition of new security requirements or solutions in the lifecycle of an application. Concepts like migration and crypto-agility are presented and discussed. The third element is the interoperability of IoT applications from a security point of view. The deliverable investigates the difference between conformance and interoperability testing. In addition, the deliverable identifies the most common approach for secure interoperability among IoT applications. For example, cross-certification in a PKI trust model or the application of trust negotiation.

Disclaimer

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 688237, but this document only reflects the consortium’s view. The European Commission is not responsible for any use that may be made of the information it contains.
## Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>04/07/2016</td>
<td>Creation. First outline proposal</td>
<td>EC JRC</td>
</tr>
<tr>
<td>0.2</td>
<td>22/10/2016</td>
<td>First draft</td>
<td>EC JRC</td>
</tr>
<tr>
<td>0.3</td>
<td>16/11/2016</td>
<td>Second draft presented at the technical meeting of ARMOUR</td>
<td>EC JRC, ODINS</td>
</tr>
<tr>
<td>0.4</td>
<td>05/01/2017</td>
<td>Updated with new sections</td>
<td>EC JRC, ODINS</td>
</tr>
<tr>
<td>0.5</td>
<td>10/01/2017</td>
<td>Updates to the schema of the European certification framework</td>
<td>EC JRC, ODINS</td>
</tr>
<tr>
<td>0.6</td>
<td>15/01/2017</td>
<td>New material related to IoT secure interoperability and other sections</td>
<td>EC JRC, ODINS</td>
</tr>
<tr>
<td>0.7</td>
<td>21/01/2017</td>
<td>Addition from SmartTesting on incremental testing</td>
<td>Smart Testing</td>
</tr>
<tr>
<td>0.8</td>
<td>23/01/2017</td>
<td>Final corrections and changes before the review</td>
<td>EC JRC</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>1.0</td>
<td>25/01/2017</td>
<td>Proof-reading and minor corrections</td>
<td>UPMC</td>
</tr>
<tr>
<td>1.1</td>
<td>12/04/2017</td>
<td>To address comments by the ARMOUR reviewers</td>
<td>JRC</td>
</tr>
</tbody>
</table>
# Table of Contents

1. **Introduction** ................................................................................................................. 8

2. **Security Certification in IoT** ......................................................................................... 10

   2.1 **An history of security certification** ........................................................................... 10

   2.2 **Current security certification schemes** ....................................................................... 12

       2.2.1 **International security certification schemes** ...................................................... 12

   2.3 **International certification schemes** ............................................................................. 12

       2.3.1 **Common Criteria** ................................................................................................ 12

       2.3.2 **The ISASecure Certification Programme** ............................................................. 16

       2.3.3 **Collaborative protection profiles** ......................................................................... 17

       2.3.4 **Information Technology Security Evaluation Criteria (ITSEC)** ...................... 18

       2.3.5 **Federal Information Processing Standards FIPS-140** ....................................... 18

       2.3.6 **Industrial Automation and Control Systems (IACS)** ....................................... 19

       2.3.7 **Common Criteria Recognition Arrangement (CCRA)** .................................... 22

       2.3.8 **SOG-IS** ............................................................................................................. 23

       2.3.9 **UL 2900 certification** ......................................................................................... 24

       2.3.10 **Secure Change** .................................................................................................. 24

   2.4 **European National Security Certification schemes** .................................................. 24

       2.4.1 **French security certification scheme** ................................................................. 24

       2.4.2 **German security certification scheme** ............................................................... 25

       2.4.3 **UK certification scheme** .................................................................................... 26

   2.5 **Relevant security standards, best practices and guidelines** ................................. 27

       2.5.1 **EN50128** ........................................................................................................... 27

       2.5.2 **IEC61508** ........................................................................................................ 28

       2.5.3 **ISO 27001/27002** ............................................................................................... 28

       2.5.4 **NIST Special Publication 800-183** ..................................................................... 28

       2.5.5 **NIST Cryptographic Standards** .......................................................................... 29
2.5.6 NIST SP 800-82 ................................................................. 29
2.5.7 DO-178B ................................................................. 29
2.5.8 IEC61508 ................................................................. 29
2.5.9 ISO 26262 ................................................................. 29
2.5.10 Multiple Independent Levels of Security/Safety (MILS) 29
2.5.11 EURO-MILS .............................................................. 30
2.5.12 IEC 62304 ................................................................. 30
2.5.13 ISO 9001 ................................................................. 30
2.5.14 The role of security standards .................................................. 30
2.6 Issues and challenges of security certification schemes ................. 30
2.7 Security and Privacy certification ....................................................... 34
2.8 A new European security certification scheme in IoT ....................... 37
  2.8.1 Problem statement ................................................................. 37
  2.8.2 Drivers for a new European certification scheme .......................... 37
  2.8.3 Key elements of the new European security certification scheme ....... 39
  2.8.4 Main roles ............................................................................. 43
  2.8.5 Description of the main flows ................................................... 44
  2.8.6 ARMOUR Model based testing (MBT), TTCN and Labelling .............. 46

3 Key elements of a design to support extendibility and flexibility of security and privacy in IoT .................................................. 49
  3.1 Introduction .............................................................................. 49
  3.2 Security certification for incremental changes ................................. 49
  3.3 Monitoring after deployment and security certification ....................... 53

4 Key elements of a design to support secure interoperability of IoT applications ...... 55
  4.1 Introduction .............................................................................. 55
  4.2 Solutions to support secure interoperability ..................................... 55
  4.3 Trust model based on Public Key Infrastructure (PKI) ....................... 56
1 Introduction

This deliverable investigates how different security and privacy solutions and products can be used in a harmonised way to support the design and deployment of secure IoT applications. In the IoT domain, this goal is more challenging than other domains because of the presence of many different heterogenous technologies and applications, which are usually implemented in a vertical manner due to market forces, boundary conditions and operational constraints. The deliverable describes three key elements for achieving this goal: the first element is to analyze the strengths and weaknesses of security certification in the IoT domain. Security certification has a long history from its origins in the defense domain (see section 2.1), but its application in the IoT domain can present challenges, which are identified and described in section 2.6. Then, a potential certification framework to address these challenges is presented. The framework is based on the concepts presented in the other deliverables of ARMOUR. The second element is to define a design, which takes in consideration the dynamicity of IoT and the definition of new security requirements or solutions in the lifecycle of an application. Concepts like migration and crypto-agility are presented and discussed. The third element is the interoperability of IoT applications from a security point of view. The deliverable investigates the difference between conformance and interoperability testing and the potential solutions to support interoperability among IoT applications/systems and devices.

This is the first deliverable of Task 4.2 in WP4. The following Table 1 shows how this deliverable addresses the different elements of Task 4.2.

Table 1 Coverage of aspects of Task 4.2 in this deliverable

<table>
<thead>
<tr>
<th>Elements of task 4.2</th>
<th>How this deliverable addresses the specific elements of task 4.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>This task investigates how different security and privacy solutions or components, which are defined in their respective systems or contexts, can be used in a harmonised way to support the design and deployment of secure IoT applications. Two main aspects will be addressed: a) IoT applications are often vertical applications developed for specific business goals and requirements. IoT applications defined in this way are usually based on vertical security and privacy solutions. For example, they may be based on a trust model (e.g., PKI) designed only for that application. It is important to provide the interoperability among IoT applications from a security and privacy point of view. For example, if the trust model of a set of applications is based on different CA and algorithms, the definition of cross-certification schema and protocols is needed to support secure interoperability.</td>
<td>Section 4 describes the main approaches and solutions to support secure interoperability among IoT applications/systems and devices.</td>
</tr>
</tbody>
</table>
This task will investigate what types of best practices or technical solutions (e.g., cross-certification) could be adopted to foster interoperability and how to test them at the level of IoT applications.

b) IoT applications are not static but they can evolve in time. Their functions can increase, become more complex or they can fade in oblivion. In the security area, some security solutions (e.g., cryptographic algorithms) which are appropriate at a specific time and context and they have been successfully tested and certified, may not be appropriate in a next version of the IoT application or some time after the IoT application was successfully deployed. For example, the validity of the cryptographic algorithms or the length of the keys is not appropriate any longer. The task will investigate how security and privacy solutions are able to support the lifecycle of IoT applications. The task will define test procedures to test and validate the migration and the extendibility of IoT applications from the security and privacy point of view, for example, the migration aspects from one release to another of the IoT application or the level of crypto-agility and flexibility.

As a first step, this deliverable describes the most common security certification frameworks including Common Criteria in sections 2.1, 2.2, 2.3 and 2.5. An analysis of the main challenges and issues with security certification and Common Criteria is presented in section 2.6. This analysis is needed in this deliverable to identify the key challenges the ARMOUR framework is trying to solve.

One of the main identified challenges is to address the dynamic aspects of IoT and the lifecycle of IoT applications.

While the detailed description of how the ARMOUR testing and certification system will support the lifecycle of IoT devices and applications will be presented in deliverable 4.3, this deliverable presents an analysis on the following key aspects for security certification in section 3:

1. Approaches to support incremental security certification for different incremental releases of IoT devices/systems/applications
2. Monitoring of certified products after deployment.

Additional elements, which are part of WP4 objectives.

A brief introduction on how security certification can address the combination of security and privacy requirements is provided in section 2.7, which will be further described in D4.5.

An overview on the key elements of a potential European security certification and labelling framework, which will be further elaborated in D4.3 and D4.5.
2 Security Certification in IoT

2.1 An history of security certification

Certification has been defined in various ways in literature. In this document, we define certification as “A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system”. This definition is extracted from NIST SP 800-37 (NIST 2010).

Security certification is needed to ensure that a product satisfies the required security requirements, which can be both proprietary requirements (i.e., defined by a company for their specific products) and market requirements (i.e., defined in procurement specifications or market standards). In the latter case, these requirements are also defined to support security interoperability. For example, to ensure that two products are able to mutually authenticate or to exchange secure messages.

Security certification is needed to ensure that products are secure against specific security attacks or that they have specific security properties.

Note that in the rest of this deliverable, the term security certification does also include certification of a product or a system against privacy requirements. We believe that the privacy certification should be part of security certification and it can be addressed with the same certification process by including additional test suites and certification steps.

The process for certification of a product is generally summed up in four phases:

1. Application. A company applies a product for evaluation to obtain a certification.

2. An evaluation is performed to obtain certification. The evaluation can be mostly done in three ways: a) the evaluation can be done internally to support self-certification. b) The evaluation can be performed by a testing company, which is legally belonging to the product company. c) It can be third party certification where the company asks a third-party company to perform the evaluation of its product.

3. In case of an internal company or a third-party company evaluation, the evaluation company provides a decision on the evaluation.

4. Surveillance. It is a periodic check on the product to ensure that the certification is still valid or it requires a new certification.

As described in (Anderson 2009), the initial efforts to define a security testing and certification framework for products originated in the Defence domain. An obvious reason was that the military systems are designed to operate in a hostile environment and must be protected against security threats, which are more likely to appear than with those systems that belong to a commercial domain. In addition, there was the need to design a system able to support different access levels for classified and non-classified information and support
interoperability. Through various phases, described in detail in (Lipner 2015), which will not be repeated here, these initial needs produced the Orange book, which provided criteria for classifying system security into a series of levels of products evaluation – C1, C2, B1, B2, B3 and A1 – depending on how carefully engineered were the mechanisms for assuring the confidentiality of classified information.

The different levels are provided in Figure 1.

D: Minimal Protection  
C1: Discretionary Security Protection  
C2: Controlled Access Protection  
B1: Labeled Security Protection  
B2: Structured Protection  
B3: Security Domains  
A1: Verified Design  
A2: Verified Implementation

*Figure 1 Levels of products evaluation in the Orange book*

Note that some of the levels (D,C1) could also be based on commercial product. At that time, mature commercial operating systems with reference to Unix were mentioned.

The Orange book was published in August 1983 and it became a requirement for ICT systems processing classified information at more than one level. As described in (Anderson 2009), while this was a valuable and needed process to support trust in government systems dealing with secure and sensitive information, the certification process was lengthy and costly. In fact, it could last 2-3 years. While, this was acceptable for the defence domain where a project or a product (e.g., a secure ICT system) could last for years and cost millions of dollars, this could be an issue for market distribution of a commercial product. The certification process also introduced a delay and certified products lagged behind the commercial state of art. In addition, the evaluation had to be performed by the National Computer Security Centre, a division of the NSA, a government agency.

A similar system was set up in Europe, which was called the Information Technology Security Evaluation Criteria (ITSEC), which eventually evolved to the Common Criteria, which is also known as ISO 15408. The Common Criteria is described in detail in section 2.2.1; here we want to identify some key elements and difference with the original Orange book.

In comparison to the Orange book, which was focused on protecting classified information, the Common Criteria is wider and permits systems and devices to be evaluate against a specific protection profile. In a similar way to the Orange book, Common Criteria also defines different levels of evaluation called Evaluation Assurance Levels (EAL) from 1 to 7.

A significant difference from the Orange book is related to the certification laboratories. As written before, the Orange book process involved a government agency for certification, while in the Common Criteria process, products can be evaluated by competent and independent licensed laboratories to determine the fulfilment of particular security properties (e.g., protection profiles) or a certain assurance level. This approach applies only to the lower assurance levels and the highest levels of certification are still performed directly by government labs.
The protection profile is based on Security Targets, which are the documents, which identify the security properties of the target of evaluation. For more details on the definition of the protection profiles, EAL and other elements of the Common Criteria see (CC 2016).

As in the case of the Orange book, the process of evaluation using Common Criteria can be quite expensive and there is an ongoing discussion if some other process could be more suited to the commercial market.

An analysis of the issues and challenges for the certification scheme is presented in section 2.6.

Regarding Privacy certifications, in recent times, a certification scheme for Privacy seals has also been put in place by EuroPrise (https://www.european-privacy-seal.eu/EPS-en/Home). The workflow and standards for privacy certification have similarities to the security certification workflow. A proposed joint certification process is proposed in section 2.7.

2.2 Current security certification schemes

2.2.1 International security certification schemes

The aim of this section is to provide an overview of the existing certification schemes. In this section, we will also identify the key standards for risk analysis, certification and labelling.

2.3 International certification schemes

Here we describe the existing international certification schemes like Common Criteria.

2.3.1 Common Criteria

The Common Criteria is also known as ISO 15408.

Common Criteria Certification provides independent, objective validation of the reliability, quality and trustworthiness of IT products. It is a standard that customers can rely on to help them make informed decisions about their IT purchases. Common Criteria sets specific information assurance goals including strict levels of integrity, confidentiality and availability for systems and data, accountability at the individual level, and assurance that all goals are met.

The Common Criteria is a descendant of the US Department of Defence Trusted Security Evaluation Criteria (TCSEC) originally in the 1970s. TCSEC was informally known as the ‘Orange Book’. Several years later Germany issued its own version, the Green Book, as did the British and the Canadians. A consolidated European standard for security evaluations, known as ITSEC, soon followed. The United States joined the Europeans to develop the first version of the international Common Criteria in 1994.

The first major CC release came in May 1998 with the release of CC 2.0 followed by version 2.1 in August 1999. CC parts 1-3 became an International Organization for Standardization (ISO) standard in 1999 (ISO/IEC 15408) followed by the CEM which became an ISO standard (ISO/IEC 18045) in 2005.
In 2007 the next significant version of the CC standard, version 3.1 was released. The current version is CC v3.1 release 4. Statistics provided by the CC international portal as of September 2014 list a grand total of 2,436 products have been certified using the Common Criteria standard (CC 2014).

The following key concepts are described here. They are extracted from (CC 2012) and (CC2014):

- A Target of Evaluation (TOE) is defined as a set of software, firmware and/or hardware possibly accompanied by guidance. While there are cases where a TOE consists of an IT product, this need not be the case. The TOE may be an IT product, a part of an IT product, a set of IT products, a unique technology that may never be made into a product, or a combination of these.

- A Protection Profile (PP) expresses an implementation-independent set of security objectives for a type or category of ICT product. It also specifies the security requirements and assurance measures which fulfil those objectives.

- A Security Target (ST) expresses security objectives of a specific ICT product and defines the functional requirements and assurance measures to fulfil those stated objectives. It also defines an implementation of the security requirements. The ST forms the basis for an evaluation and may claim conformance to one or more PPs.

- Evaluation Assurance Levels (EALs) are formed from a taxonomy of assurance classes, families, and components defined in CC standard Part 3. There are seven hierarchically ordered EALs increasing in assurance that serve to provide general-purpose assurance packages.

The EALs are defined in Figure 2.
<table>
<thead>
<tr>
<th>EAL level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Functionally Tested. Provides analysis of the security functions, using a functional and interface specification of the TOE, to understand the security behaviour. The analysis is supported by independent testing of the security functions.</td>
</tr>
<tr>
<td>2</td>
<td>Structurally Tested. Analysis of the security functions using a functional and interface specification and the high level design of the subsystems of the TOE. Independent testing of the security functions, evidence of developer &quot;black box&quot; testing, and evidence of a development search for obvious vulnerabilities.</td>
</tr>
<tr>
<td>3</td>
<td>Methodically Tested and Checked. The analysis is supported by &quot;grey box&quot; testing, selective independent confirmation of the developer test results, and evidence of a developer search for obvious vulnerabilities. Development environment controls and TOE configuration management are also required.</td>
</tr>
<tr>
<td>4</td>
<td>Methodically Designed, Tested and Reviewed. Analysis is supported by the low-level design of the modules of the TOE, and a subset of the implementation. Testing is supported by an independent search for obvious vulnerabilities. Development controls are supported by a life-cycle model, identification of tools, and automated configuration management.</td>
</tr>
<tr>
<td>5</td>
<td>Semi-formally Designed and Tested. Analysis includes all of the implementation. Assurance is supplemented by a formal model and a semiformal presentation of the functional specification and high level design, and a semiformal demonstration of correspondence. The search for vulnerabilities must ensure relative resistance to penetration attack. Covert channel analysis and modular design are also required.</td>
</tr>
<tr>
<td>6</td>
<td>Semi-formally Verified Design and Tested. Analysis is supported by a modular and layered approach to design, and a structured presentation of the implementation. The independent search for vulnerabilities must ensure high resistance to penetration attack. The search for covert channels must be systematic. Development environment and configuration management controls are further strengthened.</td>
</tr>
<tr>
<td>7</td>
<td>Formally Verified Design and Tested. The formal model is supplemented by a formal presentation of the functional specification and high level design showing correspondence. Evidence of developer &quot;white box&quot; testing and complete independent confirmation of developer test results are required. Complexity of the design must be minimised.</td>
</tr>
</tbody>
</table>

*Figure 2: Definition of EALs from Common Criteria extracted from (ECORYS 2011).*
The international community has embraced the Common Criteria through the Common Criteria Recognition Arrangement (CCRA) whereby the signers have agreed to accept the results of Common Criteria evaluations performed by other CCRA members. The National Information Assurance Partnership (NIAP) was formed to administer a security evaluation programme in the United States that utilises the Common Criteria as the standard for evaluation.

Common Criteria defines different roles (extracted from (CC 2012)):

- Consumers. The CC is written to ensure that evaluation fulfils the needs of the consumers as this is the fundamental purpose and justification for the evaluation process. Consumers can use the results of evaluations to help decide whether a TOE fulfils their security needs. These security needs are typically identified as a result of both risk analysis and policy direction. Consumers can also use the evaluation results to compare different TOEs.

- Developers. The CC is intended to support developers in preparing for and assisting in the evaluation of their TOEs and in identifying security requirements to be satisfied by those TOEs. These requirements are contained in an implementation-dependent construct termed the Security Target (ST). This ST may be based on one or more PPs to show that the ST conforms to the security requirements from consumers as laid down in those PPs.

- Evaluators. The CC contains criteria to be used by evaluators when forming judgements about the conformance of TOEs to their security requirements. The CC describes the set of general actions the evaluator is to carry out. Note that the CC does not specify procedures to be followed in carrying out those actions.

The common criteria approach is widely used in the world but it is also received criticism and suggestion for changes. See section 2.6 for additional details.

Proposal for changes to the existing Certification scheme has been raised by Chris Salter in (Salter 2011), where the following recommendations have been proposed:

1. To streamline and make more readable the common criteria documents themselves like the Protection Profile.

2. Definition of common *standard* protection profiles, which could be used for technologies and products, which have a similar set of features and they are subject to a common set of threats.

3. A tailored evaluation methodology has to be created for each technology area.

Some of the concepts from (Salter 2011) has been used in the new vision statement for the Common Criteria and CCRA is available at (CC 2012). One key aspect, which is also an element of the potential security certification scheme is the definition of collaborative Protection Profiles (“cPPs”) and supporting documents, in order to reach reasonable, comparable, reproducible and cost effective evaluation results.
2.3.2 The ISASecure Certification Programme

ISCI (ISA Security Compliance Institute) is a not-for-profit organisation incorporated by ISA in 2006 to host certification, conformance and compliance assessment activities in the automation arena. The ISASecure certification scheme was derived from the framework of the ISA99 Standards Roadmap.

As described in (ISASecure 2016), ISASecure independently certifies industrial automation and control (IAC) products and systems to ensure that they are robust against network attacks and free from known vulnerabilities. The ISASecure program is based upon the IAC security lifecycle as defined in ISA/IEC 62443. At this time, the scope of the ISASecure certifications includes assessment of off-the-shelf IAC products and IAC product development security lifecycle practices. The overall schema of ISA/IEC 62443 is shown in Figure 3.

![Figure 3: ISASecure certification scheme](image)

The Security Development Lifecycle Assurance (SDLA) certification promotes security development lifecycle practices intended to improve the quality of security in IAC systems.
ISASecure does not offer assessments for integrator site engineering practices or asset owner operations and maintenance practices. ISASecure certifies off-the-shelf systems; not the site engineered / deployed systems.

ISASecure identifies four security assurance levels (SAL) as defined in ISA/IEC 62443.

2.3.3 Collaborative protection profiles

While there are many important benefits to Common Criteria areas exist where improvement was needed:

- Twenty-six nations are signatories to the CCRA. A nation recognizing evaluations performed by other CCRA participant nations has limitations. Certificate recognition means the evaluation scheme in the certificate authorizing nation correctly performed all of the activities involved in CC and CCRA processes. This does not mean the certified ICT product met the security requirements of another CCRA participant nation.
- The requirements in the CC standard were written to be sufficiently flexible to allow specification of a wide range of ICT products. This was shown to have had an unintended effect of yielding varying and/or subjective results especially at EALs above level 2.
- The CC was devised to ensure the evaluation fulfils the need of multiple target audiences but of particular importance is the end-user (or consumer). Product evaluations with an EAL assurance level typically claim security requirements asymmetrically from one another as a common minimum bar technologies need to meet is not defined in CC. This leaves the end-user wrestling with the arduous task of finding certified ICT products that will meet their security needs. End users need to be made aware they have a voice in the process.

To address these needed improvements, the CCRA Management Committee announced in September 2012 a new-style Protection Profiles called collaborative Protection Profiles or cPPs. cPPs are developed by International Technical Communities or iTCs. cPPs move away from Protection Profiles of the past that were developed without strong engagement and endorsement of all CCRA participant nations.

There are currently four Collaborative Protection Profile: Collaborative Protection Profile for Stateful Traffic Filter Firewalls, Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, and Encryption Engine and Collaborative Protection Profile for Network Devices. The last one is the most interesting for our purpose, which TOE is a network device. It provides a minimal set of security requirements expected by all network devices that target the mitigation of a set of defined threats. All the security functional requirements specify some evaluation tests focused on the functional requirement and on one specific method of performing it, for example authentication with elliptic curves.

The TOE, as we said before, is defined as a set of software, firmware and/or hardware possibly accompanied by guidance. It could be a set of devices related to certain environment of execution, for example, home automation or industry. This is the idea we
use in D4.1, so several cPPs could be created for each specific TOE, different levels of security and different levels of certification, as we explained before with the EALs.

2.3.4 Information Technology Security Evaluation Criteria (ITSEC)
The Information Technology Security Evaluation Criteria (ITSEC) was a structured set of criteria for evaluating computer security for IT products and systems. The ITSEC was first published in May 1990 in France, Germany, the Netherlands, and the United Kingdom based on existing work in their respective countries. Following extensive international review, Version 1.2 was subsequently published in June 1991 (ITSEC 1991) by the Commission of the European Communities for operational use within evaluation and certification schemes.

The ITSEC has been largely replaced by the Common Criteria and it will not be addressed further in this deliverable.

2.3.5 Federal Information Processing Standards FIPS-140
The Federal Information Processing Standards (FIPS) are U.S. government computer security standards, which specify requirements for cryptography modules. The current version of the standard is FIPS 140-2, issued on 25 May 2001.

A brief history of FIPS-140 is following.

FIPS 140-1 was issued on 11 January 1994 and it was developed by a government and industry working group, composed of vendors and users of cryptographic equipment. The group identified four "security levels" and eleven "requirement areas" and specified requirements for each area at each level. The list of security levels and requirements areas is described below.

FIPS 140-2 was issued on 25 May 2001 and it is an updated version to take in account: a) the technology developments since 1994 in cryptographic technology and b) the comments received from the vendor, tester, and user communities. It was the main input document to the international standard ISO/IEC 19790:2006 Security requirements for cryptographic modules issued on 1 March 2006.

FIPS 140-3 is a proposed new version of the standard which is currently under development. It was initially scheduled for delivery in 2013, but the draft was subsequently abandoned. In the first draft version of the FIPS 140-3 standard, NIST introduced new features like software security section, one additional level of assurance (Level 5) and new Simple Power Analysis (SPA) and Differential Power Analysis (DPA) requirements. After the draft was abandoned, it is not clear if these new features will be maintained.

As described in (FIPS 2002), there are four security levels:

1) Security Level 1, which provides the lowest level of security. Basic security requirements are specific for a security module and no specific physical security mechanisms are required. An example of Level 1 cryptographic module is a personal computer (PC) encryption board.
2) Security Level 2 enhances the physical security mechanisms of security level 1 by adding the requirement of tamper evidence including seals or coating. The coating or seal must be broken to physically access the plaintext cryptographic keys. Security level 2 requires also a role-based authentication.

3) Security level 3 goes a step beyond level 2 by requesting to prevent the intruder from gaining access to the critical security parameters (CSP) held within the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that purges from memory all plaintext CSPs when the removable covers/doors of the cryptographic module are opened. In addition, security level 3 requires identity based authentication mechanisms, enhancing the security provided by the role based authentication mechanism specified in level 2.

4) Security level 4 provides the highest level of security in FIPS. At this security level, the physical security must provide a complete envelope of protection including the detection and response to all unauthorized attempts of physical access, which result in memory zeroing as in level 3. In addition, the cryptographic module must guarantee the same level of security even outside the normal environmental conditions for voltage and temperature.

In addition to the identified requirements, the different levels of security impose requirements on where the software and firmware components of the cryptographic module can be hosted and operate. More details are in (FIPS 2002).

While FIPS was designed specifically for cryptomodules, the scheme based on levels can also be adopted in other context, especially for the three main features of physical security, authenticated access control and hosting platform. Some of the concepts will be reused in this deliverable in the following sections.

In relation to FIPS 140, FIPS 140-2 established the Cryptographic Module Validation Program (CMVP) as a joint effort by the NIST and the Communications Security Establishment (CSEC) for the Canadian government. CMVP validates commercial cryptographic modules to the Federal Information Processing Standard (FIPS) 140-2 and other cryptography-based standards.

2.3.6 Industrial Automation and Control Systems (IACS)

“Cyber-attacks targeting industrial automation and control systems (IACS) have been perpetrated for some years already. STUXNET, the malware that affected Iranian nuclear installations, was probably climactic in raising the industrial community’s awareness of the risk that plants, their neighbourhood and customers might suffer, should a significant cyber-
attack hit them. The threat landscape indicates that the various cyber-threats targeting critical infrastructures are increasing\(^1\).

Thus, the ENISA’s recommendations\(^2\) reflected the industrial community’s need to test and certify IACS’ cyber-security in the following terms:

‘ICS manufacturers are starting to (or will have to) include security requirements in the design phase of ICS components and applications. However, operators indicate that independent evaluations and tests are missing to effectively guarantee that those devices are in fact secure and that interoperability has also been considered when the new security features/capabilities are included. Furthermore, penetration tests and white box audits in controlled laboratories have shown that there are basic security bugs in devices and applications that could be properly identified if security development good practices were included into the development cycle. In any case, manufacturers, ICS security tools and services providers, as well as operators cannot be completely aware of the implications a modification may have with respect to their own systems or third-party ones. Moreover, it is important to certify that ICS do comply with minimum quality requirements with respect to cyber-security programming bugs’.

During the last six years, in its role of flagship Project - within the European Programme for Critical Infrastructure Protection (EPCIP) - the European Reference Network for Critical Infrastructure Protection (ERNCIP) has been mainly working on the initialization and maintenance of Thematic Groups (TG) with the focus of fostering the development of more advanced security solution for Critical Infrastructures across Europe. Among the nine currently running Thematic Group, the one on Industrial Automation Control System has been established in order to explore specific issues related to cyber security. The Group, established back in 2014, has initially worked on the identification of typical IACS configurations in view to properly scan the horizon and take decision on whether to focus on the cyber security of entire systems (as integrated in the industrial environment) or of single components. The analysis of the most recurring configurations, as gathered by the group, has led to the decision to work on components’ level.

In this specific field, the Group has identified a wide gap in the European landscape, characterized by a missing framework for testing (and certifying) the cyber security of the most sensitive components installed in the IACS environment. Thanks to the mandate and sponsorship of partners Directorates General, the TG has then started working on a feasibility study for the establishment of a European Framework for the Compliance and Certification of the Cyber Security of IACS’ components.

The initial steps of a potential roadmap toward this objective have been laid down in the deliverable that describes the main pillars that constitute the core activities that had to be carried on by the Group. Among them: 1) a stakeholder consultation in order to gather consensus, recruit further experts and fine tune the initial proposal; 2) a collection and

\(^1\) More on this topic: “Proposals from the ERNCIP Thematic Group for a European IACS Components Cyber-security Compliance and Certification Scheme”, published by the European Commission’s Joint Research Centre, JRC94533, 2014, p. 9.

analysis of common cyber security requirements from existing standards; 3) the development of security profiles in order to describe the environment in which a component should operate and the desired level of cyber security; 4) the design of the compliance and certification process.

The need to undertake all of the aforementioned activities has pushed the JRC facilitators in widely promoting such effort in view to expand the Group’s network. Participation to events organized by ENISA, ETSI’s Cyber Technical Committee and CEN/CENELEC Cyber Security Coordination Group (CSCG) has led to the establishment of mutual support through the designation of observers that are taking part to the ERNCIP thematic group with the aim of supporting the project’s activities, the stakeholder consultation and the recruitment of qualified experts in the following areas: standardization, compliance and certification process, cyber security, penetration testing and manufacturing of IACS components.

The Group’s motivation in carrying on such initiative, come from an accurate analysis of the current European landscape. EU Member States are actively working on the implementation of Certification Schemes for the Cybersecurity of both IT and OT systems and components, as consolidated experiences show that certified products can contribute to the security of modern infrastructures. Many Governments have asked Information Security Agencies to define minimal technical requirements for technical standards for IT related equipment and in the upcoming years they will be looking into methods for widening these requirements and applying them also to the Industrial Automation Control Systems. This particular field requires a granular approach that should take into account the variety of components currently integrated into the industrial systems in order to assess which of them require enhanced focus and inclusion in certification schemes. As not all of the components are pivotal for the protection and security of certain infrastructures, cybersecurity-related schemes should focus on those devices and components that are in charge of vital functions that shouldn’t be lost or shouldn’t suffer disruptions.

Another aspect that should also foster the establishment of certification schemes for the cyber security of IACS' components is also the possibility that the IACS' equipment manufacturers may have an easier access to the wider European market by obtaining a certification that is valid in the entire Union. Such circumstance would avoid them to initiate a certification procedure for each of the Member States in which they’d like to offer their products. On an even wider scale, and in a later stage, the establishment of European certification framework, based on recognised technical standards, may also lead to international mutual recognitions that should enable European manufacturers to sell their products in non-EU countries without reobtaining the certification of their products twice. The work carried on by the ERNCIP TG stands as a clear use case on this specific matter as European experts are discussing the feasibility of the adoption of testing requirements from international standards such as the IEC-ISO 62443 (Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels) that is also used for the ISA secure Conformance certification (http://www.isasecure.org/en-US/) established in the USA.

The current picture of the ERNCIP TG’s work in the field of testing and certification of components, already shows the contours and the path that should lead to the establishment of a European framework in this field.
The ERNCIP’s ‘IACS Compliance & Certification Framework’ (ICCF), in fact, proposes four IACS Compliance & Certification Schemes (ICCS):

- ICCS-A1 (Compliance self-declaration);
- ICCS-A2 (Third-party compliance assessment);
- ICCS-B (Cyber resilience certification);
- ICCS-C (Full cyber resilience certification);

The rationale behind these four levels is the following:

1. Basic self-assessment only tells the customers that the vendor has checked the compliance of a product against a shared set of requirements;
2. When the same assessment is performed by an independent, accredited third party, customers are certain of the rigour of the assessment process and of the objectivity of the evaluation of the product;
3. Beyond only a formal assessment, ‘on paper’, a trusted third party tests the cyber-robustness of the product to check if it resists a set of commonly agreed tests (e.g. robustness tests);
4. Beyond scheme 3, assessing the development, operation and maintenance processes, associated with the evaluated IACS product, gives the customers even greater confidence in its cyber-security.

2.3.7 Common Criteria Recognition Arrangement (CCRA)

In the context of Common criteria, one of the issues raised in section 2.6 is the lack of harmonization of protection profiles. The objective of the CCRA (and SOG-IS described later in 2.3.8) is to enable a context where ICT products and protection profiles which earn a Common Criteria certificate can be procured or used without the need for further evaluation. This can be achieved by a mutual recognition (i.e., arrangement) whereby the signers have agreed to accept the results of Common Criteria evaluations performed by other CCRA members. The CCRA seeks to provide grounds for confidence in the reliability of the judgements on which the original certificate was based by requiring that a Certification/Validation Body (CB) issuing Common Criteria certificates should meet high and consistent standard.
Within the CCRA only evaluations up to EAL 2 are mutually recognized. The European countries within the former ITSEC agreement typically recognize higher EALs as well. Evaluations at EAL5 and above tend to involve the security requirements of the host nation’s government.

In September 2012, a majority of members of the CCRA produced a vision statement whereby mutual recognition of CC evaluated products will be lowered to EAL 2 (Including augmentation with flaw remediation). Further, this vision indicates a move away from assurance levels altogether and evaluations will be confined to conformance with Protection Profiles that have no stated assurance level. This will be achieved through technical working groups developing worldwide PPs, and as yet a transition period has not been fully determined. This evolution is in line with the framework proposed by ARMOUR where levels are actually associated to specific PP.

An authorizing nation sponsors and oversees an evaluation scheme and authorizes the CC certificates that are issued. An evaluation scheme provides the regulatory and administrative framework for laboratories or facilities within the authorizing nation to evaluate and certify ICT products. A consuming nation agrees to recognize ICT products certified by other authorizing nations. An authorizing nation is also a consuming nation.

2.3.8 SOG-IS

Participants in this Agreement are government organisations or government agencies from countries of the European Union or EFTA (European Free Trade Association), representing their country or countries.

As described in (SOGIS 2016), SOG-IS has the objective to:

1. Coordinate the standardisation of Common Criteria protection profiles and certification policies between European Certification Bodies in order to have a common position in the fast growing international CCRA group.

2. Coordinate the development of protection profiles whenever the European commission launches a directive that should be implemented in national laws as far as IT-security is involved.

For certificate producing nations there are also two levels of recognition within the agreement:

1. Certificate recognition up to EAL4 (as in CCRA)

2. Certificate recognition at higher levels for defined technical areas when schemes have been approved by the management committee for this level.
The recognition agreement is dated in January 2010 and it is available at http://www.sogis.org/uk/mra_en.html.

2.3.9 UL 2900 certification
The UL Cybersecurity Assurance Program has developed a CAP certification approach, which verifies that a product offers a reasonable level of protection against threats that may result in unintended or unauthorized access, change or disruption.

UL CAP assessment is based on the requirements of the UL 2900 Standard. UL 2900-1 and the subparts of UL 2900-2 contain product requirements that will be verified during a product assessment.

As described in (UL 2016), a product assessment verifies a product's software is in compliance with required security controls. These security controls may include, but are not limited to, role-based access control, secure data storage, cryptography, key management, authentication, integrity and confidentiality of all data received and transmitted.

The UL 2900 Standard contains minimum requirements for each of these controls. The Standard contains requirements for the vendor to design the security controls in such a way that they demonstrably satisfy the security needs of the product. The Standard also describes testing and verification requirements aimed at collecting evidence that the designed security controls are implemented.

We note that the UL 2900 standards is not published and there has been critics on this lack of visibility on the standard as mentioned in (Arstechnica 2016).

2.3.10 Secure Change
The FP7 project Secure Change (http://www.securechange.eu/) investigated and researched new approaches for security software certification with a specific focus on the changes in the product. The project developed techniques, tools, and processes that support design techniques for evolution, testing, verification, re-configuration and local analysis of evolving software. The project results were applied and evaluated to the industrial application domains of mobile devices, digital homes, and large scale air traffic management.

2.4 European National Security Certification schemes
In this section, we will present three main European certification schemes at national levels.

2.4.1 French security certification scheme
The description of the French certification schema by ANSII is derived directly from the official ANSII document (ANSSI 2015).

The French Network and Information Security Agency (ANSSI) is responsible for examining certifications according to the directives given by the certification management committee.
The security certifications performed in France, regardless of the evaluation method and besides conformance claims verifications, systematically rely on intrusion testing to establish the security assurance level reached by the product.

Certification is based on evaluation studies conducted by laboratories licensed by the French Prime minister and accredited by the French accreditation committee (COFRAC) according to the standard NF EN ISO/CEI 17025. These laboratories are commonly referred to as Information Technology Security Evaluation Facilities (ITSEF). The evaluations are conducted in accordance with specifications or standards specified by the ANSSI.

Certification mainly addresses three types of objectives. It may be required to ensure compliance with regulations, such as European or national directives. Certification may also address a contractual objective, in cases where a customer from the public or private sectors requires such a certification. Finally, software vendors or industrials may want to differentiate from the competition by certifying their product (marketing objective).

Depending on the security needs expressed by the evaluation sponsors, the French certification scheme offers two types of evaluations:

1. The Certification de Sécurité de Premier Niveau or CSPN (First Level Security Certification) is a predefined workload evaluation. Evaluation costs are therefore known in advance for a given type of product. The investment is quite limited, and the evaluation is mostly oriented towards intrusion testing, rather than conformity. Additional details on CSPN are also presented in D4.1

2. The Common Criteria evaluation allows to certify a product with various Evaluation Assurance Levels starting from EAL1 (basic attacker potential, script kiddie) up to EAL7 (high attacker potential) and takes into account the security of the development process.

2.4.2 German security certification scheme

The German security certification scheme is described in detail in (BSI 2012).

The awarding of security certificates of IT products, protection profiles and sites is governed in the BSI.

The procedure is carried out at BSI in accordance with the quality management manual and the procedural instructions of the certification body and in accordance with the standard DIN EN 45011, in accordance with the requirements of the international recognition arrangements (e.g., CCRA and SOGIS).

Certification is carried out as an application procedure. Following the preliminary assessment, the technical evaluation takes place based on the relevant evaluation criteria. The evaluation is performed by an evaluation facility approved by BSI and is technically monitored by the certification body.

The evaluation ends with a positive (pass) or negative (fail) evaluation result. The applicant is notified based on this vote. If the evaluation result is positive, the certificate and the
certification report will be enclosed with the notice. The applicant may give notice of appeal against the notice.

In the case of a positive completion of the certification, the certification report will also be published on the BSI website, unless publication has been explicitly objected to.

Note that there are two types of certifications: system certifications and product certifications.

BSI uses the Common Criteria approach for certification. BSI develops protection profiles in order to define national security requirements in provisions for evaluation. Protection profiles are evaluated and certified in order to confirm their conformity with the concepts of the respective evaluation criteria.

2.4.3 UK certification scheme
The UK security certification scheme is presented in (CESG 2016) and the following key concepts are extracted from that reference and provided here:

The evaluation criteria currently recognised by the UK certification scheme, and the methodologies associated with them, are:

1. the Common Criteria (CC) ISO/IEC 15408 and the Common Methodology For IT Security Evaluation (CEM) ISO/IEC 18045;

2. the IT Security Evaluation Criteria (ITSEC) and the IT Security Evaluation Manual (ITSEM)

CESG, as the UK’s National Technical Authority for Information Assurance, operates the Scheme as part of its Industry Enabling Services (IES).

The UK security certification scheme presented in (CESG 2016) also identifies key roles. While this is background information, it is important to describe it here because similar roles will be adopted in the report:

- Senior management team. The CESG Senior Management Team provides the CB with top level direction, setting and reviewing policy and monitoring the performance of the Scheme overall.

- Commercial Evaluation Facilities (CLEFs), which carry out the evaluations, and the establishment of approved techniques and procedures. CLEF is also accredited as a testing laboratory by UKAS, against ISO/IEC 17025.

- Certification body, which appoints CLEFs and keeps their appointment under review. It also confirms the suitability of each Target of Evaluation (TOE), certifying the results of evaluations conducted under the Scheme, and publishing details of certified products and PPs on the CESG and Common Criteria Portal websites. The certification body also deals with the appropriate national and international agencies regarding the mutual recognition of certificates.
- Sponsors, which refers to the person or organisation that requests and funds an evaluation and a certification; and is entitled to receive the reports produced.

- Developers, which refers to the person or organisation that has designed, developed, implemented, tested, manufactured and produced the TOE.

- The term ‘Vendor’ refers to the person or organisation that sells and distributes the TOE to consumers.

- Procurement body, which refers to the person or organisation that purchases and acquires the TOE for use in an operational environment.

- Accréditor, refers to the person or organisation that is responsible for the overall security of a System in its operational environment and who takes into consideration the conclusions and recommendations of the product’s Certification Report, when assessing residual risks to the System.

(CESG 2016) also defines the overall process, which is divided into Preparation, Evaluation and Certification and Assurance Maintenance phases. Details on the process are not described in this section, but key elements of the process are referred in other sections.

### 2.5 Relevant security standards, best practices and guidelines

#### 2.5.1 EN50128

This standard does concern itself both with security and safety certification of software, and follows IEC61508. In particular, it specifies procedures and technical requirements for the development of programmable electronic systems for use in railway control and protection applications. It is more focused on safety rather than security as it addresses the need to guarantee the operations of critical components like safety signalling in addition to non-critical components like management information systems.

It is applicable exclusively to software testing and the interaction between software and the system of which it is part.

As in other standards, different levels of security certification are defined. They are called Security Integration Levels (SIL) and they are mapped to test coverage levels (R stands for "recommended", HR stands for "highly recommended") as for table
Table 2: Security Integration Levels in coverage levels in EN50128 (from EN50128 standard)

<table>
<thead>
<tr>
<th></th>
<th>SIL 0</th>
<th>SIL 1</th>
<th>SIL 2</th>
<th>SIL 3</th>
<th>SIL 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Statement Coverage</td>
<td>R</td>
<td>HR</td>
<td>HR</td>
<td>HR</td>
<td>HR</td>
</tr>
<tr>
<td>2. Branch Coverage</td>
<td>-</td>
<td>R</td>
<td>R</td>
<td>HR</td>
<td>HR</td>
</tr>
<tr>
<td>3. Composed conditions (MC/DC or MCC-Coverage)</td>
<td>-</td>
<td>R</td>
<td>R</td>
<td>HR</td>
<td>HR</td>
</tr>
<tr>
<td>4. Data Flow Analysis</td>
<td>-</td>
<td>R</td>
<td>R</td>
<td>HR</td>
<td>HR</td>
</tr>
<tr>
<td>5. Path Coverage</td>
<td>-</td>
<td>R</td>
<td>R</td>
<td>HR</td>
<td>HR</td>
</tr>
</tbody>
</table>

2.5.2 IEC61508
This standard covers functional safety and it is aimed at the electro technical industry. It provides a methodology to assess the risks to systems and determine the safety requirements, and introduces both safety integrity levels and the safety lifecycle. It supports the certification of components for use in safety-critical systems. However, its focus is on bounding failure probabilities, and it does not consider penetration testing or attacks from a malicious adversary.

2.5.3 ISO 27001/27002
ISO 27001 sets out to “provide requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS)” while 27002 has a list of possible controls. Essentially, these documents provide a framework for a large organization that seeks to measure and evaluate how well it does information security management; they make it susceptible to internal and external audit processes, and are basically seen as audit checklists. However, they are fundamentally about companies securing their own assets and operations, not about making products that protect their customers.

As a consequence, these standards are not relevant for the specific focus of security certification of products, but they could have a role for the security certification of systems.

2.5.4 NIST Special Publication 800-183
This special publication on `Networks of `Things" is closest to the subject matter of this paper. It sets out a framework for analysing security in IoT in terms of
ve primitives (e.g., sensors, aggregators, communication channels, eUtilities and decision triggers). Its contribution is at the level of architecture and terminology, as an aid to security analysis, rather than anything directly testable. However, it gives some idea of the potential complexity and the range of other standards and tests that may be necessary in building and certifying an IoT system.

2.5.5 NIST Cryptographic Standards
The US National Institute of Standards and Technology (NIST) has since the 1970s developed a series of standards for cryptographic algorithms, modes of operation and protocols, starting with the Data Encryption Standard (DES) in the 1970s, followed thirty years later by the Advanced Encryption Standard (AES) and secure hash algorithms. These are very widely used. Adherence to standards is not however sufficient for security as implementations should usually run in constant time to forestall side-channel attacks, as noted above.

2.5.6 NIST SP 800-82
This is a best practice for the secure deployment of Industrial Control Systems (ICS). It is aimed at deployment, and concerns itself with network architecture and the use of security features such as firewalls for protection. It is not as applicable to programming ICS systems securely.

2.5.7 DO-178B
This standard concerns itself with software intended for use in airborne vehicles and the certification of devices. The primary aim is to ensure software is tested for safety critical purposes. Thus, it is intended more to protect from error and mischance than from malice.

2.5.8 IEC61508
This standard covers functional safety, is aimed at the electro-technical industry (though used elsewhere too), and is at a higher level than EN50128. It provides a methodology to assess the risks to systems and determine the safety requirements, and introduces both safety integrity levels and the safety lifecycle. It supports the certification of components for use in safety-critical systems.

2.5.9 ISO 26262
Another standard that follows on from IEC 61598, this standard is about to the functional safety of road vehicles. It does cover the full lifecycle of development, but does not refer to best practices for security.

2.5.10 Multiple Independent Levels of Security/Safety (MILS)
The MILS specification does concern itself with both safety and security, but applies mainly to operating system design in general. It can be used in combination with Common Criteria techniques, but is more of a design principle than a testable standard. It is good at preventing certain types of vulnerabilities, but is agnostic about others, assuming they are the user’s responsibility.
2.5.11 EURO-MILS

This standard takes into account virtualisation and kernel isolation in much the same way as MILS. It is meant for both safety and security, but is also slow and cumbersome to test against. Primarily useful for high assurance systems like aircraft, defense, and intelligence purposes, but too expensive for IoT devices.

2.5.12 IEC 62304

This standard is devoted to the total software lifecycle of medical devices. It does recognize that software of unknown origin should be vetted with a risk-based approach, and not be used if at all possible, but is a self-policing strategy at heart.

2.5.13 ISO 9001

This standard is relied on by a number of the above standards. It is a general quality assurance standard about the repeatability of a firm's management processes, with a systems approach to management, factual decision-making and a commitment to continuous improvement.

2.5.14 The role of security standards

There are many security standards with specify the security functions or properties in many different domains including IoT. A survey on the security standards of IoT is provided in (Granjal 2015). A detailed description of the security standards of IoT is out of scope of this deliverable as the focus is only on standards related to security certification, which are described in this section above. Security standards could be used in the security certification process by a company to declare conformance of its product to a specific security standard, but this may not be enough to obtain a label. A security certification process (like the one described in ARMOUR deliverables) must be put in place and executed to demonstrate that the product fulfills the security requirements defined in the test. In addition, conformance to a standard does not ensure secure interoperability among IoT devices and applications.

2.6 Issues and challenges of security certification schemes

The objective of this section is to describe the main issues and challenges of the existing certification schemes, which have been described in the previous sections.

While the Common Criteria approach is one of the most used approaches for security certification, it has been criticized by various stakeholders.

Table 3 identified the main issues and criticisms of the Common Criteria approach from literature. A summary and analysis will follow this table.

Disclaimer: The statements in the Description column in the table are extracted from the references identified in the Source column. This deliverable does not directly endorse these statements even if they are used as an input to the analysis.
<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
<th>Source</th>
<th>Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>In theory, countries that recognize Common Criteria evaluations should have considerable clout for convincing vendors to make security improvements to products. In practice, these countries have not cooperated sufficiently to agree upon requirements and many participants do not require the evaluations. The current trend is for countries to create their own testing regimens. In some cases, these competing evaluation schemes will be used to protect indigenous industries, and, more disconcertingly, as an opportunity to force vendors to disclose sensitive information.</td>
<td>(NCSA 2011)</td>
<td>Lack of mutual recognition</td>
</tr>
<tr>
<td>2.</td>
<td>Common Criteria does not define the features or functionality that a product must have or require that the product itself be secure. Instead, the development of the product is evaluated against a security target, which can be a protection profile developed by a user or a company statement of what the product is intended to do. These are evaluated against a set of security assurance requirements to determine if the development process for the product enables it to meet its claimed security functionality. Basically, it tries to determine if the product does what it says it will do. This approach is a strength and a weakness of Common Criteria. By not specifying functionality requirements, it is a flexible framework that can be applied across a broad spectrum of products. But it focuses on process rather than product. Knowing what a product is designed to do does not necessarily mean it can do it well or securely, critics say.</td>
<td>(Jackson 2007)</td>
<td>Lack of transparency</td>
</tr>
<tr>
<td>3.</td>
<td>No single set of criteria can be used to produce comparable and effective evaluations for a wide range of technologies</td>
<td>(NCSA 2011)</td>
<td>Lack of mutual recognition</td>
</tr>
<tr>
<td>4.</td>
<td>The CC evaluation process for lower assurance levels (EAL1 to EAL4), which correspond to the levels at which most products are evaluated, are essentially a paper evaluation of the development process and product documentation, not requiring evaluation of software.</td>
<td>(ECORYS 2011)</td>
<td>Lack of coverage</td>
</tr>
<tr>
<td>5.</td>
<td>Commonly used protection profiles often do not correspond to the functionality requirements actually required by users.</td>
<td>(ECORYS 2011)</td>
<td>Lack of transparency</td>
</tr>
<tr>
<td>6.</td>
<td>Long and expensive. CC evaluation life cycle is lengthy and expensive. In fact, due to the complexity of the process and the high cost, vendors have to spend a large e ort on preparation for the evaluation, which adds to the cost and time of the evaluation itself. High assurance level (as EAL4) certification can take 12 years, and, often, by</td>
<td>(Kaluvuri 2014)</td>
<td>Cost of the security certification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>the time the process is completed a new version of product is already delivered.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>7.</strong> Concerns for Mutual Recognition. Though the CC scheme is a widely recognized international standard, there are several concerns regarding the consistency of the assessments by the evaluating laboratories located in different countries, since the Common Criteria Recognition Arrangement (CCRA) does not prescribe any monitoring and auditing capability. In addition, the relevance of CC certification for governmental institutions, specific national interests can impact the impartiality of the assessment. (Kaluvuri 2014)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lack of mutual recognition</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>8.</strong> Point in time certification. CC certifies a particular version of the product in certain configurations. Any changes to the configuration or any updates to the product that affect the Target of Evaluation (TOE), which is the part of the product that is evaluated, invalidate the certification. This is not a desirable situation, given that products evolve and are updated at a frantic pace and the certification must not be frozen to a specific version of the product. (Kaluvuri 2014)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lack of support for product lifecycle</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>9.</strong> Comparability. One of the main objectives of CC is to allow consumers to compare certified products on the market in an objective way from a security point of view. However, certification documents are filled with legalese and technical jargon. Hence, comparison is not straightforward nor easy. (Kaluvuri 2014)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lack of transparency</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>10.</strong> The above discussion should have shown how the Common Criteria are not well matched to the needs of the control systems world. At the technical level, a security certification scheme must be able to cope with dynamic systems, dynamic threats and real users working in real organisations. It must complement, rather than conflict with, existing safety certification mechanisms. But above all, its function is to provide assurance to asset owners that the systems and components they buy from the vendor community are fit for purpose. (Anderson 2009)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lack of transparency</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lack of support for product lifecycle</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>11.</strong> Common Criteria fail to deal satisfactorily with systems that are patched frequently, as operating systems now are; observers of the operating-system patching cycle and vulnerability scene have come to the conclusion that the Common Criteria are no more than a bureaucratic exercise whose costs far outweigh the benefits. (Anderson 2009)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lack of support for product lifecycle</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>12.</strong> How has this CC-evaluated product improved my IT system’s security? The problem is that few, if any, metrics exist to support this question, and without them, it’s impossible to assess the cost–benefit ratio for performing an evaluation. The CC government members believe that evaluated products provide better protection than unevaluated products, and that evaluated products contribute to overall system security when integrated into systems. Yet, without a system-level approach to security, and the metrics to (Hearn 2004)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lack of transparency</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security composition</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
support such an approach, these views lack a solid foundation.

| 13. | Other significant obstacles and barriers include concerns about the comparability and competency of evaluations. Conflicts between international harmonization and national investments could be especially significant if major European nations and the US continue to follow increasingly divergent paths as they pursue national interests. Although the founding member nations were able to work through their differences to produce the CC and the CC Recognition Arrangement (CCRA), living with the result proves once again that the devil is in the (implementation) details. | (Hearn 2004) | Lack of mutual recognition |

| 14. | CC are not suitable for services e.g. Cloud and big data. This is an example of why certification of components alone is not enough; we need an overall framework for certification which includes services, personnel, systems and products as well. | (ENISA 2014) | Security composition |

| 15. | It is an open question if existing applications might continue running on top of certified, and properly modified of course, products. Assessments should take place to this direction. Re-writing existing application will prove to be a big challenge. | (ENISA 2014) | Lack of support for product lifecycle |

| 16. | Re-certification after changes being made in the product is not mandatory, but should be considered case by case | (ENISA 2014) | Lack of support for product lifecycle |

| 17. | Testing what the vendor wants tested rather than what the customer (or other relying party) needs tested is a pervasive problem with the Common Criteria. | (Anderson 2009) | Lack of transparency |

| 18. | Common Criteria assurance requirements tend to be inspired by the traditional waterfall software development methodology, while most of the modern software is produced using modern agile paradigms. | (Beznosov 2004) | Lack of support for product lifecycle |

The key issues (fourth column of table Table 3) are summarized here:

1. **Lack of mutual recognition.** Security certification may not be equivalent due to different reasons (not mutually recognized protection profiles, different configuration)
2. **Lack of transparency.** The security certification may not give a clear idea to the end user for the expected level of security the product provides.
3. **Lack of coverage.** Security certification may not cover all the security requirements and threats an user has to address.
4. **Cost of the security certification.** The cost of the security certification process can be quite high and it can significantly impact the business model of the producer.
5. **Lack of support for product lifecycle.** Security certification is usually done against a static version of the product and its operative environment and they can both change in time. This can be especially true in the Internet of Things environment.
Security composition. It is not guaranteed that security properties of products can be composed in a system. Then, it cannot be assumed that a system is more secure because it is based on a composition of security certified products.

A new security certification scheme or the evolution of an existing one should be able to address the challenges identified in Table 3. The elements of a new certification scheme based on the findings and solutions of the ARMOUR project are described in section 2.8.

2.7 Security and Privacy certification

The concept of privacy certification is not new, even if security certification (or safety certification) has been historically the main priority. European Commission’s General Data Protection Regulation (EU 2016b) in Recital 77 encourages the “establishment of certification mechanisms, data protection seals and marks” to enhance transparency, legal compliance and to permit data subjects [individuals] the means to make quick assessments of the level of data protection of relevant products and services.

A relevant case study for Privacy certification is the concept of Privacy Seal (EU 2013). The Privacy seal is a trans-European privacy trust mark issued by an independent third party certifying compliance with the European regulations on privacy and data protection. See (see https://www.european-privacy-seal.eu/ by EuroPriSe for more information on the Privacy Seal and the activities carried out by EuroPriSe. The Privacy seal concept is relatively similar to the label concept of security certification where the label is the seal itself.

The overall process to obtain a Privacy Seal could also be similar to envisaged security certification process. Private and public manufacturers of IT products and IT-based services can apply for the certificate of the European seal. The trust mark is awarded after successful evaluation of the product or service by independent experts and a validation of the evaluation by an impartial certification authority.

Reference (EU 2013) provides and extensive description of the most common Privacy Certification processes available in the world. One of the main examples is TRUSTe, which defines processes for Privacy certifications for various products and services. In (TRUSTe 2016) are defined Privacy certification standards for Smart Grids, Enterprise and others. TRUSTe works closely with stakeholders to identify the needs for the definition of new Privacy certification standards. The standards define the Privacy Program requirements, the vendor must satisfy in its service or product. Examples of requirements defined in the TRUSTe standards are related to protection against phishing or the implementation of encryption methods for data protection and data confidentiality.

These examples already show that security certification and privacy certification cannot be disjointed but they should be combined as they often address the same or similar requirements (e.g., access control, confidentiality) or solutions (e.g., cryptographic algorithms).

We can identify the main challenges for privacy certification in the context of this deliverable:
1) Privacy certification standards are highly fragmented both in the privacy context (e.g., various companies providing privacy certification for seals) and the public context (e.g., European national states)

2) The language used in the definition of the requirements is not harmonized across the entities providing the privacy seal. As a consequence, privacy certification suffers the same issue of security certification: lack of interoperability and mutual recognition for the security certification. In addition, we do not identify (at the time of writing this deliverable) initiatives to define harmonization actions like SOG-IS in the privacy area apart from EuroPriSe.

3) At the time of writing this deliverable, the seal is only a binary value: Yes or Not, while the security certification foresees different levels of certification. As reported in (IAPP 2016), the U.K. Information Commissioner's Office suggested that a traffic-light-style graded scale, to indicate levels of data protection could be implemented.

The authors of this deliverable believe that such challenges could be addressed using a similar framework already defined for security certification. A critical aspect would be the integration of security and privacy requirements in the same process even if the initial drivers and sources of requirements would be different.

A possible workflow for the integration and security and privacy requirements would be as described in Figure 5.

The concept is the EDPS, Application Experts and the European Governing board work together to support the definition of the security and privacy requirements, which will be used by the Protection Profile producers. As a consequence, the privacy standards and requirements used to drive the Privacy Seal, will become part of the overall protection profile and the privacy seal is part of the final Label.
In this flow, the accreditation of test beds for privacy seals discussed in (EC 2013) would be part of the already existing accreditation process for security certification.

In fact, the section policy option proposed in (EC 2013b) for privacy seals is focused on the incorporation of the EU data protection requirements into an existing EU certification scheme, which is the same approach identified here.
2.8 A new European security certification scheme in IoT

2.8.1 Problem statement
From the analysis of the international and European national security certification schemes presented in 2.3 and 2.4, it is clear that the Common Criteria is endorsed by the main European national bodies and international organizations even if there are some proposal for complementary security frameworks. For instance, the France government does also support Certification de Sécurité de Premier Niveau (CSPN) described in ARMOUR deliverable 4.1 even if the Common Criteria is widely supported.

Then, the starting point for a European wide security certification process is the Common Criteria but the main issues, which have been highlighted before must be addressed.

From the analysis provided in Table 3, we can identify the following main issues:

1. **Re-certification and patching.** Re-certification of an already certified system or product is an issue raised in items 8,9,11, 16 and 18. This requires the definition of a new process or a modification of the existing approach for Common Criteria. A discussion on the advantages of using MBT and TTCN v3.0 to support a more efficient re-certification and patching process is presented in section 3.

2. **Mutual Recognition.** Mutual recognition of the certification or comparability of protection profile is an issue raised in items 1,3,7,13. While, this is an important matter, the existing CCRA and SOG-IS are already addressing this matter.

3. **Security and trust coverage.** Security certification with Common Criteria may not be enough to provide full security and trust of a product. This is suggested in items 2,4,5,14.

4. **Certification costs.** Common criteria certification is considered a long and expensive process, which does not make it suitable for fast market deployment or relative short product cycles as in the consumer market (see section 3.4.2). This was raised in item 6.

5. **Non-applicability to specific products and systems.** Some classes of system and products are difficult to certify due their intrinsic features and characteristics. This issue was raised in item 14.

6. **Comparability and visibility of the certification.** Users do not have a clear metric of comparison among different certified products.

7. **Usability.** The Common criteria certification does not give a clear and simple indication to the users of the provided level of trust. Metrics are missing for this purpose. This issue was raised in item 12.

2.8.2 Drivers for a new European certification scheme
The need for a European certification scheme has already been suggested by various studies including (ECORYS 2011) and (ERNCIP 2014).
In particular, (ERNCIP 2014) highlighted the need for a European certification scheme for industrial components for the main reasons:

1. Need to harmonize the current national certification schemes (Germany, UK and France) but there are others to create a common European certification scheme based on a common approach.

2. Testing and certifying the cyber-security of IACS components/devices seemed to IACS stakeholders a useful step to take as it would bring a higher level of cyber-confidence to industry buyers and users.

3. The need to establish a practical scheme guaranteeing mutual recognition of certificates across Europe and compatible with similar requirements beyond. This aspect is complementary to item 1. Note that the current collaboration schemes like CERA and SOG-IS could be a starting point for the establishment of a common format and semantic of the certificates.

4. A common European certification scheme would bring a higher level of cyber-confidence to industry buyers and users.

We note that item 4 could be a key enabler to improve the competitiveness of the European industry because a harmonized certified device and product at European level could become an added value for cybersecurity products and a recognized label at global level (e.g., similar to the CE marking). As described in (ECORYS 2011), EU certification may be more widely recognised as an international ‘quality label’ and, hence, support the international competitiveness of European producers. It must be recognised however, that non-European producers that obtained the same European certification would benefit in an equal way from this ‘quality label’.

In a similar way, the ECORYS report (ECORYS 2011) defined the following drivers. Note that (ECORYS 2011) makes a distinction between Type 1 and Type 2 security products. The Type 1 products represents general security products as for the mass or consumer market, while the Type 2 products represents specific high level security products like the ones used for public safety or homeland security contexts. Note that (ECORYS 2011) uses the term Conformity Assessment and Certification (CAC) to define the certification process.

1. Reduce barriers to trade in security products within the EU for Type 1 security products. Reduce fragmentation of EU markets for security products within the EU and promote a ‘level playing field’ for security products within the EU.

2. Reduce the burden of security requirements for certification of security products both for Type 1 and Type 2 for security manufacturers because they will have only a harmonized certification procedure across Europe.

3. Support for existing or future security policy needs and ensure common minimum performance levels for security products in EU. For example, an existing policy for security products in the road transportation sector or the energy sector could benefit from a European security certification scheme, which could be directly linked to it. An important example is the new Radio Equipment Directive (RED 2014), where links can be established between the certification of the wireless device and its security certification.
In addition, to the identified drivers, we highlight the advantage of a common European certification scheme for security certification of personnel working in the cybersecurity industry because the procedures and processes would be the same or quite similar (at European level).

Another important advantage would be the harmonization of the security testing tools and systems used for the testing and certification process, which can reduce market fragmentation. At the moment, there are many different security certification tools for various purposes, which increase the costs and make more complex the activity of security testing workshops and certification centres. By harmonizing the certification procedures, these issues can be removed or mitigated.

2.8.3 Key elements of the new European security certification scheme

Here we describe the key elements of a potential European security certification scheme, which can overcome the issues defined in section 2.6 and address the drivers identified in section 2.8.2.

The key elements of this scheme are following:

1. A common European security certification scheme and the accompanying standard.
   On the basis of the analysis of the national certification scheme described in 2.4 we note that there is a convergence to the Common Criteria approach even if this is not formally decided. While there have been various attempts to propose new security certification approaches, we believe that the widespread use of common criteria at global level is a strong supportive element to propose common criteria as the basis of the European security certification scheme. Still, some elements of other proposed security frameworks like CSPN could be adopted in the proposed security certification scheme. CSPN (Coutant 2016) is proposed by the French security agency ANSI. The typical CSPN evaluation consists of 25 days dedicated to software security. A description of the CSPN process is provided in D4.1.

2. A certification scheme based on different certification levels. As proposed in (ECORYS 2011) and (ERNCIP 2014), certification can be of different levels where the basic level is a self-certification and it is not mandatory, while higher levels require that the certification is executed in a security certification centre with different types of test (see section 2.3.6 for a description of the IACS levels). This approach is consistent with the Evaluation Assurance Levels (EAL) of Common Criteria.

3. Labelling scheme. A labelling scheme can be created to give a straightforward indication on the level of certified security of a product. This process is similar to what proposed by the French ANSSI where the label is associated to a successful certification.

4. Harmonized protection profiles at European level. The SOG-IS agreement could be extended to define harmonized protection profiles in specific domains (i.e., a separate protection profile for each domain). Harmonized protection profiles at European level for devices and products are needed to support a common certification process. Harmonized protection profiles are also needed to support the labelling concept because labels must be associated to a specific protection profile,
which is the same across Europe. Harmonized protection profiles should be defined to address the issue of security and trust coverage. With the term domain, we mean a set of applications with common security requirements, which can be used to drive the definition of a common protection profile.

5. **Evolution of Common Criteria.** While the Common Criteria can be the basis for a European security certification process, some of the issues identified in section 2.6 must be addressed. In particular, the definition of a process to address changes in the protection profile is one of the highest priority tasks. The following sub-recommendations are proposed (which are similar to what proposed in (Salter 2011) (CC 2012))

- Common set of protection profiles (“standard protection profile”) for technologies and products, which have a similar set of features and they are subject to a common set of threats.
- A lightweight scheme to address incremental or evolutionary changes in the products. From this point of view, the approach proposed by the French ANSSI, which is called CSPN could be used to complement the CC approach, anticipate it or apply only for specific types of products. For example, consumer mass market IoT products

6. **Accredited European security certification centres.** A network of European security certification centres must be set-up to support a European security certification scheme. An accreditation process must also be defined for the same purpose. In this area, the Future Internet Research and Experimentation (FIRE) initiative could be exploited to support this network. While the FIRE was not designed to become an operational instrument for testing and certification of a wide range of products, the types of tests and experience acquired in FIRE could be used in the specific domain of IoT, where some aspects of IoT security and security certification could be quite novel in comparison to conventional ICT systems. In other words, the lessons learnt in the development of the FIRE test bed should be taken in consideration when the accreditation procedures for the European security certification centres should be designed.

7. **European Governing board.** A European governing board to support the European security certification scheme should be established to manage changes in the European security certification scheme and to coordinate aspects related to the European harmonization (e.g., harmonization of the protection profiles in each domain). See also (ECORYS 2011) for a similar recommendation of an EU body for security compliance and certification. One of the objectives of the European governing board is also to address gaps in the certification of the security products and to address requests from the community (e.g., service providers, government, users, manufacturers) for the need of the definition of new harmonized protection profiles.

8. **Model Based Testing and TTCN.** The adoption of formal models to represent the IoT product and system can be used not only to automate and improve the efficiency of the security certification process but also to define the key security properties and how they interact.
These elements can address the issues of the existing certification schemes identified in section 2.6 as described in the following table:

**Table 4: Elements of the new European security certification scheme to address the issues identified in 2.6.**

<table>
<thead>
<tr>
<th>Key elements</th>
<th>Issues</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>A common European security certification scheme and the accompanying standard.</td>
<td>Lack of mutual recognition</td>
<td>By creating a common European security certification scheme, mutual recognition is ensured.</td>
</tr>
<tr>
<td>Certification scheme based on different certification levels</td>
<td>Cost of the security certification</td>
<td>By adopting different levels of certification, the manufacturers can choose the most cost-effective security certification scheme for their products.</td>
</tr>
<tr>
<td>Labelling scheme</td>
<td>Lack of transparency</td>
<td>A labelling scheme linked to specific protection profiles can give a clear indication on the type of security certification to which the product has been submitted. The labels does also give an indication on the security and trust coverage of the product.</td>
</tr>
<tr>
<td>Harmonized protection profiles</td>
<td>Lack of mutual recognition</td>
<td>Harmonized protection profiles can support both mutual recognition and the labelling scheme to support the Comparability and visibility of the certification.</td>
</tr>
<tr>
<td>Evolution of Common Criteria</td>
<td>Lack of support for product lifecycle</td>
<td>The Common criteria process should be enhanced to address in a more efficient way the re-certification of an already certified product.</td>
</tr>
<tr>
<td>Accredited European security certification centres</td>
<td>Lack of mutual recognition</td>
<td>Accredited European security certification centres are a key element to guarantee an harmonized security certification process.</td>
</tr>
<tr>
<td>European Governing board</td>
<td>Lack of mutual recognition</td>
<td>The board will ensure European harmonization of the security certification process to support mutual recognition.</td>
</tr>
<tr>
<td>Lack of coverage</td>
<td>The board will also address gaps and requests from stakeholders to mitigate the risk of non-applicability to specific products and systems.</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Model Based Testing and TTCN</td>
<td>Security composition Cost of the security certification</td>
<td>Formal models to represent the IoT products and systems can be used to automate and improve the efficiency of the security certification process but also to define the key security properties and how they interact in a IoT system.</td>
</tr>
</tbody>
</table>

The development and deployment of a new European security certification scheme based on these elements could be a step-by-step approach regulated by appropriate EU framework. The challenge is to resolve the dependencies among the different elements in a coordinated way. For example, the accredited European security certification centers would require the definition of common standards and common EU-wide protection profiles in the different domains, before they can start to test and certify products.

An important element of the European security certification process is the benchmarking and the definition of appropriate benchmarks and metrics. In particular, micro-benchmarks and macro-benchmarks could be defined as described in deliverable D4.1:

- **Micro-benchmarks**: provide useful information to understand the performance of subsystems associated with an IoT device, which are useful to identify possible performance bottlenecks at architecture level.
- **Macro-benchmarks**: provide statistics relating to a specific function at application level and may consist of multiple component-level elements working together to perform an application layer.

A more extensive analysis on micro-benchmarks and macro-benchmarks is provided in deliverable D4.1.

A preliminary pictorial description on how the different key elements of the European security certification scheme are linked is provided in Figure 6.
2.8.4 Main roles
Here we describe the possible roles for a European certification scheme.

- **Product Manufacturer.** This is the manufacturer of the product to be submitted for certification. Manufacturers can be present in different domains or a single domain (e.g., road transportation or energy).

- **EU standardization bodies.** They are responsible to define the standards (including test standards), which are used to support the definition of the test suites to be executed in the security certification process. They can also be responsible for the definition of the test bed requirements and configuration.

- **European accreditation bodies and auditors.** They are responsible for the accreditation of the certification centres and the periodic auditing.

- **European Data Protection Board (EDPB),** which is responsible to support the definition of privacy requirements and elements of the harmonized protection profiles.

- **European Governing Board (EGB),** which is responsible for managing the overall security certification process at the Europe level. The European Governing board is composed at least by the representatives of the national certification bodies and the European Commission. SOG-IS will also be part of the European Governing Board. The EGB is responsible for drafting and managing changes to the security
certification process. An entity subject to the authority of the EGB is the Labelling Program Authority, which is described below.

- The Labelling Program Authority is the European (or member state entity), which is responsible for realising the labels after a successful certification process. The Labelling Program authority associates the certification environment, test suites, tools and processes to specific labels, which are then provided to the applicant/manufacturer after a product submission. More details on the labelling concept and the role of the labelling program authority are provided in 2.8.6.

- Accredited certification centres. An accredited certification centre performs the test execution on the basis of the pre-defined harmonized protection profile. Note that existing test beds could be used. A number of firms in Europe have been certified as Commercial Licensed Evaluation Facilities (CLEFs) under the Common Criteria, and do certification work that is recognised across participating states. They mostly evaluate software products for government use, though there is some work on products such as smartcards that are sold into the banking industry.

- Harmonized Protection Profile producers. They are responsible for drafting the harmonized protection profiles at European level. The producers can be public or private bodies with expertise in security certification.

- Users. They are the users of the certified product. They use the label information as a metric to drive their procurement process. Users can be citizen, public (e.g., government) or private companies.

- European Commission. The European Commission could be part of the EGB to drive future evolutions of the certification framework. In addition, some parts of the EC could have a more operational role regarding some functions of the certification framework. For example, the publication of the documents describing the overall process and the list of accredited third parties test lab at any given moment.

2.8.5 Description of the main flows

In this table, we describe the main flows among the entities participating to the potential security certification framework. The table should be read from left to right, where the flow of action is performed by the entity on the left column to the entity in the right column. For example, the auditors perform the accreditation of an Accredited Certification Centre.

<p>| Table 5: Relationships among the main roles in the European security certification framework |
|-----------------------------------------------|-----------------------------------------------|-----------------------------------------------|-----------------------------------------------|-----------------------------------------------|-----------------------------------------------|-----------------------------------------------|
| EGB                                           | SOG-IS                                       | Auditors                                      | Accredited Certification Centre                | Manufacturers                                  | Users                                         | Producers of PP                              |
| EGB                                           | Communications with SOG-IS on the need to modify part of the procedures of the security | Define the process for accreditation.          | Defines the relationships between labels and the related | In cooperation with manufacturers, defines the need for the creation of new | Promote awareness campaigns on the usefulness of the label concept and | Defines the relationships between labels and the related protection profiles. |</p>
<table>
<thead>
<tr>
<th>Role</th>
<th>Action</th>
<th>New Protection Profiles (PP)</th>
<th>How to Apply Them</th>
<th>Anticipates the Need for the Creation of New PP for Specific Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOG-IS</td>
<td>SOG-IS is part of EGB and contributes to the activities of EGB</td>
<td>Communications the harmonized protection profiles.</td>
<td>Accept the requests by manufacturers for security certification.</td>
<td>Examines the new formulated PP for approval and acceptance in the harmonization process.</td>
</tr>
<tr>
<td>Auditors</td>
<td>Provide feedback on gaps or issues in the security certification framework.</td>
<td></td>
<td>Audit and perform accreditation of a certification centre.</td>
<td></td>
</tr>
<tr>
<td>Accredited Certification Centre</td>
<td>Provide documents to Auditors for accreditation.</td>
<td></td>
<td>Perform security certification on the products submitted by manufacturers.</td>
<td></td>
</tr>
<tr>
<td>Manufacturers</td>
<td>Provide feedback on the security certification framework.</td>
<td></td>
<td>Provide products to be certified.</td>
<td>Collaborate with PP producers for the drafting of PP.</td>
</tr>
<tr>
<td>Auditors</td>
<td>Provide feedback on the security certification framework</td>
<td></td>
<td>Perform the accreditation of certification centres.</td>
<td></td>
</tr>
<tr>
<td>Producers of PP</td>
<td>Provide feedback on the security certification framework</td>
<td>Submit the PP to the SOG-IS for evaluation.</td>
<td>Collaborate with manufacturers for the definition of PP.</td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td>Provide feedback on the security certification framework</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2.8.6 ARMOUR Model based testing (MBT), TTCN and Labelling

This section has the objective to investigate the application of formal and theoretical tools for testing. Research bodies have long investigated the application of formal methods for testing and many examples are provided in the research literature.

Deliverable D2.2 investigates and describes the application of formal methods for testing combined with Testing and Test Control Notation (TTCN) v3 language to support security certification for IoT devices.

The overall framework is described in Figure 7. The framework is based on the Model-Based Testing (MBT) approach, which has shown their benefits and usefulness for systematic compliance testing of systems that undergo specific standards that define the functional and security requirements of the system.

The structure of the system is modeled by UML class diagrams, while the systems behavior is expressed in Object Constraint Language (OCL) pre- and postconditions. Functional tests are obtained by applying a structural coverage of the OCL code describing the operations of the SUT (functional requirements). This approach in the context of security testing is complemented by dynamic test selection criteria called Test Purposes that make it possible to generate additional tests that would not be produced by a structural test selection criterion, for instance misuse of the system (Model-Based Security Functional Testing) and vulnerability tests, trying to bypass existing security mechanisms (Model-Based Vulnerability Testing). These two approaches generate a set of test cases that is stored into a database and then executed on the IoT system under test. In the ARMOUR project, the tests are defined using the TTCN v.3 language, which has been widely used for many years (in the previous versions) to test large communication systems.

The advantages of using MBT in combination with TTCN are the following:

1. The automation of the test supports a faster and more uniform testing.
2. The adoption of MBT supports a formal definition of the tests and the security requirements, which drives the certification. In addition, they can be used to support harmonization of the tests for security certification.

MBT and TTCN-3 suites can be linked directly to the labelling concept described in the other sections of this deliverable.

The idea is that a set of MBT, TTCN-3 suites, a specific configuration set and the results of the test/certification all contributes to the Label definition.

Then, the process of obtain a label for a product is described in Figure 8.

**Figure 8: Process for label request and provision**

In this process, an applicant submits a product to obtain a label. The applicant could provide the following documentation:

1. A description of the product, preferably formalized in the form of an MBT model.
2. The level of testing/assurance requested.
3. The identifier of the related harmonized protection profile to be used for the evaluation (if Common Criteria is used as a security standard). The harmonized protection profile is obviously related to the requested level of testing/assurance.
4. The domain or configuration environment where the product must be tested.
On the basis of the requested label, the test bed uses a pre-defined set of testing material, based on the ARMOUR Testing Framework (described in D2.2) which includes:

1. Model of the product to be tested based on the ARMOUR MBT approach. It would be preferable that the applicant itself defines a model of the product and submits it to the testing bed as written before. Otherwise, a testing engineer can define the MBT model on the basis of the information provided by the manufacturer and pre-existing model. The model is completed with security test patterns on the basis of the requested level of security evaluation.
2. Description of the test environment, which can be part of the MBT model or a complementary document.
3. The test suite of TTCN-3 associated to MBT.
4. The set of required testing tools to execute the test, which have been defined by the labelling program authority for all test beds on the basis of the specific requests (e.g., labels).

Then, the test bed allows the testing of the submitted product. If the test execution is successful, the test bed notifies the labelling program authority that a label can be released to the producer of the IoT device.

Note that this process is performed with a test bed external to the manufacturer. The manufacturer can also decide to perform a self-certification by using its own laboratory. In this case, the resulting label will provide this information.

The label is based on different dimensions:

1. Domain and configuration environment where the IoT device is deployed.
2. Certification level (linked to a specific protection profile)
3. How the certification is performed: self-certification or using an external test bed.
3 Key elements of a design to support extendibility and flexibility of security and privacy in IoT

3.1 Introduction

The aim of this section is to conduct an analysis, identify and describe potential approaches to support security certification after the initial security certification and deployment in the market of IoT devices or systems.

As described in section 2.6, one of the challenges identified by academia and industry in relation to security certification is how to manage small incremental changes in the IoT products. Any change to certified IoT products and its certified configuration would require a new security certification. On the other side, a complete security certification is often a very complex and costly process, which may not be feasible to implement for any small and incremental change of IoT products. As a consequence, there is a need to propose new certification process or tailor existing ones to support incremental changes. One of these change is software patching or new software releases of an IoT product, which may happen quite frequently.

Another approach recently advocated for IoT (CISCO 2016) and (CISCO 2016b) is to monitor the operations of IoT products and devices after market deployment. Because many IoT devices may not be able to implement effective security solutions and they may become the weak link in more complex IoT applications, a potential approach is to monitor anomalies in the IoT systems composed by IoT devices to identify security attacks or malicious activities. The post-mortem analysis can be used to feedback the security certification process and identify potential certification gaps. In section 3.3, a survey and analysis of the main trade-offs is presented for these aspects.

3.2 Security certification for incremental changes

This section addresses one of the main challenges identified in section 2.6: the re-certification of already security certified products due to updates like software patches. As described in (Anderson 2009) and (Kaluwari 2014).

As described in (Kaluwari 2014), “the CC scheme certifies products at a point in time, that is, certification applies to a particular version of the product and in a certain set of configurations. But products do need to evolve - either to provide new functionalities or to fix problems or both. And in such cases, the CC certification does not apply to the new version and the whole product has to undergo the certification all over again which is once again a very time consuming and expensive process, especially when the changes made to the product are very minor”

The designers of the CC scheme have tried to address this issue. In fact, to avoid such situations, the CC scheme allows products to be under the CC Maintenance Agreement (CCMA) where only the changes made to the product are evaluated.

In a similar way, as described in (NIAP 2016a), the applicant of an IT product must initiate the assurance maintenance process after the Certificate has been issued. This process requires re-evaluation of the IT product if the vendor has made a major change. The document is issued by the National Information Assurance Partnership (NIAP). NIAP is the
U.S. government organization established by NIST and NSA to maintain and operate the Scheme for the U.S. Government and to oversee and validate the evaluations performed by the accredited labs.

The description of the process is provided in (NIAP 2016b), where the main elements of the process are described:

- Definition of a security target for the changed TOE (with tracked changes).
- Impact Analysis Report (IAR) with a description of the impacts to the product and a classification for severity (minor, major).

The IAR is examined by NIAP to evaluate if the set of changes is minor or major according to the following workflow.

As part of the NIAP review process, NIAP may decide if the product requires re-evaluation because there are major changes described in the IAR or if there is no need of a re-evaluation. In the case of minor changes, the NIAP can issue an Assurance Continuity Maintenance Report (ACMR) and maintain the existing certificate.

A similar process can also be put in place in a European framework for security certification. There is the need of a central body, which takes the role of NIAP.

While the NIAP process facilitates the management of certified IoT products in the market because minor changes (once approved by NIAP) does not need to be re-certified and the issue of an ACMR is enough to keep the security certification, there is still the problem to effectively manage a re-evaluation.

The findings from (Kaluvari 2014) show that the total percentage of products that are under the maintenance agreement is just 22 % of all the certified products. In addition, there are few requests for re-evaluation. Then, the authors of (Kaluvari 2014) concluded that the large majority of products are certified only once at the beginning. As described in (Anderson 2009), one of the reasons is related to the cost of re-evaluation. Manufacturers are fearful of subject themselves to another long and costly re-evaluation process.

The problem could be mitigated if the differences between releases of the product could be assessed in a formal and more efficient way than what it is done now. In this context, the ARMOUR project could provide solutions or mitigate this issue through the proposed approach based on Model Based Testing (MBT) and TTCN described in section 2.8.6. By defining a model of the IoT product to be certified (or the TOE in Common Criteria language), the effort of the re-evaluation could be focused on identifying the specific changes using MBT and then producing the associated tests in TTCN.

The additional advantage would be that the concept of IAR or a similar document in an European Certification process could be formalized using MBT.

An example of the concepts developed in the ARMOUR project and applied to re-evaluation is shown in the following paragraphs.
A new version of a TOE may contain new developed features or simply evolutions of the code, for instance improvements of functions, performance, bug corrections etc. All these evolutions require review on the security impacts, which may lead to a re-certification.

Based on the evidence updated for the TOE, for instance the MBT model, ARMOUR tackles finely the issue on the re-certification and helps the review of security impact using a safe regression testing techniques. Safe regression testing techniques make possible to select test cases for execution relevant for testing the modified TOE without omitting test cases that may reveal faults (Graves 2001).
The re-evaluation of a TOE is based on a comparison between the initial and the updated version of the TOE’s evidence. Several elements being part of the TOE’s evidence may evolve:

- the model (the TOE’s functional specification has evolved)
- the security patterns (new security properties are tested for the same TOE, for instance to reach a higher label)
- both may evolve (as the changes in the security test patterns are often due to the development of new functionalities in the TOE)

The test tool based on an automated comparison of the TOE’s formal evidence expressed in the form of an MBT model) can detect if there are any impacted security properties. Based on the analysis it will:

- select a set of existing test cases that are impacted by the updated TOE’s evidence
- generate new tests to cover any new or evolved security test pattern
- report on impacted vulnerability patterns, which ensure traceability to the security properties part of the security certification.

These output elements of the ARMOUR Testing Framework will serve as facilities to easy and lower the cost of the re-certification, specifically in the activities from 3 to 6, illustrated in Figure 9. The systematic and automated process offered by the framework will on the one hand easy the decision process on the need for re-certification, as it will report on the impacted security test cases and thus impacted security properties. On the other hand, only a sub-set of the test cases will be executed on the test bed and analysed, which lowers the processing and post processing part as well.

A well-known case study for the issue of security re-certification is related to the update of software in IoT devices. Today, ICT products and devices (including IoT) are often updated with new software versions and configuration. In many cases, these software updates are implemented to resolve security issues, which were not identified in the testing phases or they were related to zero-day threats. On the other side, these software updates can also generate new security vulnerabilities and issues. An additional problem is to prevent the installation and activation of malicious software in the IoT device using the same mechanism. One technology that is used in the IT industry to ensure the validity of the installed software before it is activated is to store certificates in a TPM (trusted platform module) implemented in the IoT device and check the signature of the software with the certificate. In other words, the TPM acts as an internal (to the IoT) trust anchor, which compare the digital signature of the downloaded version with the certificate. If the digital signature is successfully validated, the software can be activated and executed.

This process is also related to the after security certification post monitoring process described in the next section. The overall process for digitally signing the new software version and distributing the certificates should be linked to the security certification process. The details on how these processes are linked are not in the scope of this deliverable, but they will be described in the deliverable D4.5: Study of security and privacy aspects in IoT application lifecycle.
3.3 Monitoring after deployment and security certification

Security certification is an important element to build trust in IoT products/systems/applications but it is disputable if it can reach full coverage.

Historically the owner of a device was responsible for maintaining it. As time went on and technology became more complex, vendor after-sales organisations and third-party maintainers have started to play a role, along with regulators. The process of patching and upgrading is part of the lifecycle of the IoT device. Even if an efficient re-certification process is put in place (as discussed in the previous section), it is not guaranteed that it resolves all the security issues. In other words, as time goes by, patching alone may not be enough. In a world of complex systems, we can expect more incidents where (as with infusion pumps) each vendor can blame others for a safety incompatibility that kills. It may not be sufficient to certify the safety and security of individual components; we have to test, certify and monitor whole systems. It is already accepted that we certify a whole car, not just its component engine, brakes, steering and so on. It is also accepted that driver training and road design are linked standards. Similarly, once we have millions of autonomous, semi-autonomous and manually-driven vehicles sharing the roads, the safety authorities had better have the authority to look at the whole picture. A similar analysis can be applied to smart city applications or infrastructures.

In addition, IoT applications could also be composed by IoT products, which are not security certified. These products could become the vulnerability of the overall IoT application even if it is mostly built on security certified products. Furthermore, security IoT certification may not include the testing of zero-day vulnerabilities and threats, which were not know at the time of security certification.

A complementary (rather than alternative) approach to support IoT lifecycle of products is to introduce post-market monitoring of IoT devices. In this approach, a monitoring system is set up to collect data (management data or traffic data), which can be used to identify security threats. This approach is not a new concept; actually, fault management or misbehaviour detection system in ICT based infrastructures (e.g., energy, telecommunication) had fulfilled a similar role for many dozens of years.

In other context, this monitoring approach can be implemented using an Audit Management process. In the context of ICT security, audit is a review and examination of logs in order to test the characteristics of security procedures, to ensure compliance with established access policy and operational procedures, and to recommend any necessary changes (Pulkkinen 2007). The audit process can be linked to the model (from MBT) of the components of the ICT systems. If the audit detects a deviation from the valid and certified model, an alert is generated to trigger an investigation on the ICT systems. An important function of the audit management process is to ensure that the versions of the software and configuration settings in the various components of the ICT systems is conformant to the correct model. In other words, the audit management process should check and track any violation that certified SWs is replaced by a software version, which was not certified or it is not coherent with the security certification of an ICT system or product.

The audit management process defined in general in ICT, could be applied to the more specific case of IoT, with some caveats. Recent analysis of security and privacy aspects in IoT have highlighted the possibility to use monitoring solutions and capabilities (Yan 2014),
to enhance the overall security of IoT deployment. The challenging aspects (as reported by (Yan 2014)) and others is the scalability and heterogeneity of IoT deployments, which can reach thousands of devices with different technologies or data format. From a semantically point of view, it is also difficult to compare set of data from different IoT devices. Still, in some context like the automotive and the industry sectors where the operational requirements are usually coherent and similar across devices, the deployment of such monitoring systems could be more effective.

The potential approaches for IoT have been proposed by various authors and industry representatives as in (CISCO 2016) and (Dickson 2016). One of the key concepts is to use machine learning techniques to identify anomalies in the behaviour of IoT deployments once they have reached a point of stability. This means that very dynamic IoT deployments or IoT deployments which are not fully formed, may not receive the benefit of this approach. Machine Learning algorithms based on the management and traffic data originating from IoT devices can be used to identify known security threats (e.g., using supervised learning algorithms) or by identifying anomalies or outliers in normal behaviour (e.g., using one class classifiers). The execution of machine learning algorithms could be not hosted on the IoT devices themselves because of their limited computing or processing capabilities but a cloud based approach could be used, taking in consideration that cloud-based IoT deployment will be growing in the future.

A monitoring system could exploit a formal representation of the IoT application as provided by the UML schema used in MBT in ARMOUR. The UML/MBT representation of the IoT application could be used as input to the logic of the monitoring system to evaluate the potential vulnerabilities. The results from after market monitoring could also be used to feed a new iteration of the certification process because the reported threats could be used to enhance the MBT model and generate new TTCN test cases.
4 Key elements of a design to support secure interoperability of IoT applications

4.1 Introduction

Even if single IoT applications can be designed and deployed in a secure way, there is often the need to support secure interoperability among them. Various approaches have been proposed in literature, which will be discussed in this section. These approaches include more extensive testing to cover interoperability aspects and/or technical or organizational solutions to support secure interoperability and secure exchange of data.

There are two main aspects, which will be discussed in this section:

1) Identification and description of technical or organizational solutions to support secure interoperability.
2) An analysis of the difference between conformance testing and interoperability testing from a security point of view. While two different applications/systems/products can pass a conformance test against a single set of specifications and standards, it is not guaranteed that they are interoperable. Interoperability tests are needed to ensure that the two applications/systems/products are also interoperable.

4.2 Solutions to support secure interoperability

In this section, we identify and describe the main security solutions to support interoperability. The key idea is to support mutual trust among applications designed with different security solutions either at the level of different cryptographic algorithms or security approaches (e.g., absence or presence of cryptographic solutions).

This is often the case in ICT development and deployment: applications are designed with specific security requirements and solutions due to specific business drivers or categories or responsible. On the other side of the coin, vertical applications may need to interoperate and exchange information or request for operations for additional and overarching applications. The paradigm of the Smart City shows clearly this need. To foster an effective and secure deployment of Smart City applications, different vertical applications already deployed or under deployment, need to interoperate in a secure way.

The following approaches and solutions are identified, which will be discussed and described in the following sections:

1) Trust model based on Public Key Infrastructure (PKI).
2) Trust Negotiation
3) Secure multi-party computation (SMC)
4) Distributed Role Based Access Control (RBAC)
5) Federated Identity Management Systems.

These solutions have been identified from different sources ((Grandison 2000), (Zheng 2014), (Winslett 2002), (Miorandi 2012), (Gubbi 2013)).
Note that security is a wide concept, which includes various security functions, which are summarized here (the list is derived from (Zheng 2014) and other sources). The focus is on the security interoperability for IoT products/applications/systems as this is the context of ARMOUR.

1) Trust relationship and decision (TRD): trust management provides an effective way to evaluate trust relationships of the IoT entities and assist them to make a wise decision to communicate and collaborate with each other.

2) Privacy preservation (PP): user privacy including user data and personal information should be flexibly preserved according to the policy and expectation of IoT users.

3) Data transmission and communication trust (DTCT): data should be transmitted and communicated securely in the IoT system. Unauthorized system entities cannot access private data of others in data communications and transmission.

4) Availability. Security interoperability should be available at all time or most of the time as defined in related service level agreements (SLA).

5) Identity Trust. The identifiers of IoT system entities are well managed for the purpose of trustworthy IoT. Scalable and efficient identity management in IoT is expected.

Each of the solutions or approaches described in the list above may fulfil all these security functions or only some of them. A summary table in a subsequent section will describe on how the different solutions may fulfil secure interoperability.

4.3 Trust model based on Public Key Infrastructure (PKI)

The use of asymmetric key cryptography in a Public Key Infrastructure (PKI) is a classical way to establish trust among different ICT infrastructures or among the entities participating to an ICT infrastructure. In both cases, the concept is to use asymmetric key cryptography and digital signatures to establish mutual trust among.

A Public Key Infrastructure (PKI) is the key management environment for public key information of a public key cryptographic system. Detailed information on PKI concepts can be found in (Adams 2003) and some of the content described in this section is derived from these references.

We identify the following main components in a PKI system:

- A certificate authority (CA) that both issues and verifies the digital certificates. This is main chief of trust. CA can have a hierarchical structure.
- A registration authority which accepts and verifies the identity of users requesting information from the CA. Once the user’s identity has been authenticated the request is then forwarded to the CA. The CA will in many cases trust requests received via the RA without further validation.
- A central directory or certificate repository, which is a secure location in which to store and index keys/certificates.
- Certificate Distribution System, to distribute the certificates.
- Policies. There are policies defined for the management of the PKI system or the generation and distribution of certificates. These can be subcategorized into Certificate Policies, which put requirements on the end-entities that must be met in
order to obtain certificates, and Certification Practice Statements, which are statements by a CA operator about the practices they will follow to ensure correct outcomes.

IoT applications already developed and deployed in the field and which already support asymmetric Key cryptography can be made interoperable by developing a cross-certification trust model.

Different structures for trust model are possible as described in (Adams 2003), (Lopez 2010), (Alterman, P. 2001) and (Perlman 1999). Note that this is only a brief description and the reader can refer to the cited references for details.

- A single Root CA, where a single root CA is created to support different PKI infrastructures. The different PKI infrastructures should share the same elements of the certificate policy like certificate structure and cryptographic algorithms. This can be a heavy limitation because already deployed vertical IoT applications based on the different PKIs may have problems to support the same root CA (see (Alterman, P. 2001) and (Perlman 1999)). One organizational issue is that a central entity must be identified to implement and deploy the root CA, which may not be an easy task. A government can take up this role, but in case of global IoT applications, this can be difficult to achieve.

- Federation of Cross-certified Root CAs, where no root CA is present but each Root CAs cross-certify with each other (sign each other certificates) to establish trust relationships. If there are many root CAs, this approach would be difficult to scale.

- The Bridge CA is based on a special trust model sometimes referred to as the “hub and spoke” model. In this case, a central bridge CA can act as a “trusted” bridge CA between existing CAs. The advantage in comparison to the root CA model is that there is no need to have the same set of security certificates but the bridge CA can act as a bridge and mediate between different PKI implementations. There are case studies in e-government where this was the preferred solution (see (Alterman, P. 2001)). As in the case of the root CA, the challenge is to identify an entity, which can be responsible for setting up a bridge CA. While, there are known examples of bridge CA in the banking sector or the eGovernment, it is not known yet in the IoT domain.

- Certificate Trust List. In this trust model CAs do not establish a trust relationship between them and there are no certification paths in this architecture, but only certificates. Entities (IoT application/devices and systems) must maintain a list of CAs that they trust. This is usually done by creating a signed list of certificates, which is related to all the trusted root CAs in the system. The CTL trust model is widely deployed for web applications because of its flexibility. For same reasons, it could be the most appropriated solution to support secure interoperability for IoT applications.

One key issue is how to deploy the certificates in the IoT devices especially when a new root CA is added or removed from the trust model. This can happen due to the revocation of a root CA or the appearance of new root CA. This issue is part of a wider discussion on the Key management and distribution of certificates in IoT devices. This can be quite
challenging not only because it would require continuous connectivity for key management purposes (which means that the connection should be protected for integrity purposes) but also for storage and processing needs.

4.4 Trust Negotiation

Trust Negotiation (TN) consists of iteratively disclosing certified digital credentials. These credentials verify properties of their holders to establish mutual trust. Thus, TN deals with concepts such as formulating security policies and credentials, determining whether particular sets of credentials satisfy the relevant policies, and deferring trust to third parties (from (Bertino 2004)).

Trust Negotiation has been extensively studied by researchers in the last 10/15 years for it application in various context like web applications, critical infrastructures and so on.

The main concept is that two or more parties can exchange digital credentials to gradually build trust. The digital credentials are statements certified by given entities who verify the properties of their holders. Another definition is that digital credentials are assertions describing one or more properties about a given subject, referred to as the owner, certified by trusted third parties. Trust is thus incrementally built by iteratively disclosing digital credentials according to ad hoc resources—namely, disclosure policies. (Bertino 2004). Digital credentials can be signed with a cryptographic algorithm (e.g., a PKI) or other means.

There is an extensive literature on Trust Negotiation applied to different domains like web applications (Winslett 2002), critical infrastructures (Braghin 2010) and so on. Then, its applicability to IoT applications could be investigated further. Due to potential long negotiation process, Trust Negotiation may be not appropriate for IoT devices themselves, but rather to IoT applications like a Smart City context.

4.5 Distributed Role Based Access Control (RBAC)

RBAC models in a distributed context have also been proposed to support secure interoperability among different domains or ICT applications. There is an extensive literature on this topic. One of the drivers for the recommendation to use RBAC is that other identified solutions like PKI are not directly able to provide access control to resources or data and a Role Based Access Control could be more suited to this purpose (Joshi 2001). While many distributed RBAC models have been proposed in literature, there are still a number of key challenges to be resolved. As described in (Shafiq 2005), conflicts may arise among the RBAC policies of individual ICT (or future IoT) applications.

Conflicts, which can hamper the interoperability and the interoperability among different applications can be classified to four types according to (Shafiq 2005): 1. modality conflicts, 2. multiple management, 3. cyclic inheritance, and 4. separation of duties (SoD).

1. Modality conflicts in a policy arise because of the existence of both positive and negative authorizations for a given subject-object pair. If the proposed interoperability model does not accept negative authorizations, this conflict is mitigated.

2. Multiple management conflicts occur when multiple administrators (e.g., belonging to different applications) having authority over a common set of subjects and objects, specify conflicting authorizations in their respective policies.
3. Cyclic inheritance conflicts mainly occur in interoperation of systems employing multilevel security policies. If the interoperability model does not support multi-level security policies, this conflict is also mitigated.

4. Separation of duties (SoD) prevent two or more subjects from accessing an object that lies within their conflict of interests or disallow a subject from accessing conflicting objects or permissions, e.g., the same managers cannot authorize payments and sign the payment checks.

An additional issue is the different definitions of RBAC models or roles across different IoT applications. Each IoT application may have (and it is usually the case) defined specific roles and permissions, which are not semantically equal to other IoT applications.

The resolution of these misalignments would require:

1. the harmonization of roles and permissions among all the different IoT applications, which can very difficult to achieve and to maintain in time unless a common catalog of roles and permissions is defined through a standardization activity.
2. the definition of a central bridge or gateway, which takes the role of translating roles and permission across different applications.

### 4.6 Federated Identity Management Systems

As described in (Miorandi 2012), (Roman 2013) and (Fremantle 2014), the interoperability among IoT devices and applications require and also need to provide some mechanisms for achieving universal authentication. Without authentication, it will not be possible to assure that the data flow produced by a certain entity contains what it is supposed to contain. Another important aspect related to authentication is authorization. If there is no access control whatsoever, everything will be accessed by everyone, which is neither viable nor realistic. Identification and authentication can be implemented by using different solutions derived from interoperability of web applications or ICT applications. The need for Identity Management and interoperability in IoT was also recommended by the Expert Group on the Internet of Things (IoT-EG) (http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1752)

Federated Identity Management systems have been already proposed in literature for ICT system or web applications. The European projects STORK I and STORK II (https://www.eid-stork.eu/) had the objective to establish a European eID Interoperability Platform to allow citizens to establish new e-relations across borders, just by presenting their national eID. The results from the STORK projects could also be used to foster identity management in IoT, even if this application has not been investigated in detail to the knowledge of the authors of this report.

Because of the specific features of IoT devices, the design of federated identity management systems for IoT interoperability should take in consideration the limited processing capabilities of IoT devices in term of processing power, storage and so on.

(Fremantle 2014) has proposed the combination of OAuth 2.0 Framework with MQTT to support secure interoperability among IoT devices. The proposal has been implemented and validated using IoT devices (e.g., Arduino based boards). The authors in (Fremantle 2014) do also make a set of recommendations, which are reported here:
• The need for a clear standardization of where to put the token as well as limiting the OAuth2 token size to some reasonable limit - at least for IoT use.
• The need to define a clear MQTT flow for refresh and avoid refreshing the refresh token.
• A formal model and proof of security attributes for the use of OAuth2 with MQTT and in particular, the refresh flow, would be beneficial.
• It would be valuable to analyse the performance of this model and understand the extra cost of using OAuth2 compared with traditional security.

Even with these limitations, which can be addressed with future standardization work, the authors in (Fremantle 2014) are relatively confident that the combination of OAuth 2.0 Framework with MQTT can be used with success to support secure interoperability among IoT devices.

The IETF has published a draft guidance on security considerations for IoT (Morchon 2013), which discusses both the bootstrapping of identity and the issues of privacy-aware identification. One key aspect of the draft is the definition of a Host Identity Protocol (HIP), which is designed to provide a cryptographically secured endpoint to replace the use of IP addresses, which solves a significant problem – IP-address spoofing – in the Internet. A lighter version of HIP called Diet HIP (Moskowitz 2012) is specifically designed for IoT and M2M interactions. As discussed in (Fremantle 2014), while HIP and Diet HIP can solve difficult problems, they may have significant disadvantages for deployment. Firstly, they require low-level changes within the IP stack to implement. Secondly, as they replace traditional IP addressing they require a major change in many existing systems to work. In addition, neither HIP nor Diet HIP address the issues of federated authorization and delegation (from (Fremantle 2014)).

The authors in (Skarmeta 2015) do also recommend PANA (see (Forsberg 2008)) to support secure M2M communications during their operation. PANA can be used in combination with EAP-TLS as authentication protocols and it widely supported by the ZigBee Alliance. The use of PANA is based on identity certificates (e.g. a X.509 certificate), which contain a set of attributes associated with the smart object (e.g. manufacturer or hardware features).

Idemix (Camenisch 2002) is a cryptographic protocol suite for privacy-preserving authentication and transfer of certified attributes. It allows user authentication without divulging any personal data. Thus, no personal data is collected that needs to be protected, managed, and treated according to complex legal regulations. Nevertheless, service providers can rest assured that their access restrictions are fully satisfied. Idemix is based on the Camenisch-Lysyanskaya (CL) signature scheme, which allows to prove the possession of a signature avoiding the disclosure of underlying messages, or even the signature itself, by using zero-knowledge proofs.

The advantage of Idemix is that it provides the authentication function while protecting the privacy of the user. Idemix has been proposed for its deployment in IoT in (Hernández-Ramos 2015) among other sources.

4.7 Block chain

Another possibility to establish trust relationships among IoT applications is through the Block Chain concept. At this moment, this possibility is rather speculative and there are no
extended studies on the application of Block Chain to IoT applications. A recent report by the UK government (UK 2016) has suggested the potential of Block Chain for Trust and Interoperability. The potential application to the Energy domain is proposed. The report recommends that further studies and tests are needed before this approach is taken in consideration in the deployment of ICT applications in general and IoT specifically.

Recently, the authors of (Christidis 2016) have proposed the application of Block Chain to establish smart contracts in a Smart City environment. The authors propose to use blockchains to support a distributed peer-to-peer network where non-trusting members can interact with each other without a trusted intermediary, in a verifiable manner. Smart contract is a computerized transaction protocol that executes the terms of a contract. Smart contracts can be used to establish trust relationships. Without entering in detail in the proposal described in (Christidis 2016), the authors suggest various issues to be addressed in the deployment of block chains for IoT: a) include fail-safe mechanisms in the code to prevent dead-ends, b) improve the performance as blockchain solutions will generally underperform, resulting in lower transaction processing throughput and higher latencies, c) some blockchain solutions or functions are resource intensive so their applicability on resource-constrained IoT devices might be limited. Further work is needed in this area.

4.8 Analysis

Various technical solutions have been proposed in literature for secure interoperability among IoT devices/applications. From a testing and security certification point of view, the proposed solutions should be tested and evaluated on the basis of different parameters like scalability, performance, storage and so on.

From an organizational point of view, some of the proposed solutions (e.g., root CA in PKI) requires the definition of a central authority to support secure interoperability. This may be difficult to achieve, taking in consideration the large amount (which will be probably grow in the future) of IoT devices and applications. As a consequence, a centralized approach could be appropriate only for large IoT applications or infrastructures (e.g., cloud based) or in large and well defined scenarios like Smart City.

In addition, not all the proposed solutions are able to support security properties identified in section 4.2. Some solutions are more appropriate than others to support specific properties while others may have weaknesses, which can be exploited by security and privacy attackers. For example, Idemix supports the privacy of users in a more effective way than a basic implementation of a PKI. This is the reason why pseudonyms certificates are created in the specific domain of cooperative intelligent transport systems based on PKI to mitigate privacy risks. In other cases, an approach based on Trust Negotiation can support trust relationships among IoT applications with a higher level of granularity than a conventional PKI. On other side, these differences and disadvantages are not so evident, because each approach and solution has been refined and expanded in recent year to address the initial weaknesses.

Some solutions like trust negotiation or block chain may require long transactions or a considerable number of transactions to build trust relationships. In the IoT context, the limitations of IoT devices must also be taken in consideration.
<table>
<thead>
<tr>
<th>Solution</th>
<th>Strengths</th>
<th>Weaknesses</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust model based on Public Key Infrastructure (PKI)</td>
<td>PKI is a well-known and mature technology, widely used in my ICT systems in the world</td>
<td>The set-up and management of a PKI can be quite complex, especially in IoT environment where the management of key/certificates can be challenging.</td>
<td>To research the application of traditional PKI models to the specific features of IoT.</td>
</tr>
<tr>
<td>Trust Negotiation</td>
<td>Support for full distributed systems like IoT. It is possible to define various levels of trust on the basis of the attributes and capabilities of the IoT devices.</td>
<td>Trust negotiation can be less time efficient than other solutions (e.g., PKI) because of the long convergence time to assess the mutual trust. This can be a significant issue in IoT</td>
<td>Investigate the applicability of trust negotiation for specific aspects or domains of IoT. For example, if trust management could be more suited for IoT applications rather than IoT devices.</td>
</tr>
<tr>
<td>Distributed Role Based Access Control (RBAC)</td>
<td>RBAC is a well known and mature technology, widely used in my ICT systems in the world</td>
<td>RBAC can provide access control but it would not be able to support other security properties (e.g., integrity) and it should be complemented with other solutions. Roles can also be different across IoT applications.</td>
<td>Investigate complementary solutions, which can extend the coverage of RBAC in IoT. Support standardization processes in IoT to harmonize roles.</td>
</tr>
<tr>
<td>Federated Identity Management Systems</td>
<td>This solution supports well a distributed environment. The solution has reached maturity</td>
<td>The deployment of this solution can be still complex for the distribution of the keys.</td>
<td>Deployment aspects in a practical scenario should be investigated more in detail.</td>
</tr>
</tbody>
</table>
and many authors have proposed this solution for IoT.

The additional advantage is that this solution supports privacy in a stronger way than other solutions.

| Block Chain | Block chain is now a mature solution in the finance business and it has started to be proposed in other domains as well (e.g., energy) | The computational and storage costs of this solution is significant, which makes it not viable for the specific IoT devices. | The application of block chain to IoT is still in a pre-mature phase. Even if its applicability is limited to IoT applications and not IoT devices, the recommendation is to support additional research for block chain in IoT. |
5 Conclusions

This deliverable addressed different areas related to security certification, which has long history in the last 40 years. While Common Criteria is the most widely used security certification framework, a number of issues and challenges have been identified, which limit its use in specific contexts. This deliverable has identified the challenges and it has investigated how some of them can be removed or mitigated using the framework proposed in ARMOUR. In particular, the definition of models using MBT and test suites using TTCN-3 can be used to improve the re-certification after a patching process or an update of an IoT device. This deliverable does also present the key elements and roles of a European security certification and labelling framework, which will be further developed in other deliverables of the ARMOUR project (e.g., D4.3). The framework is based on existing entities and organizations like SOG-IS or accredited test beds for security certification for common criteria. New entities must instead be formed for new functions like labelling or governance of the framework. The deliverable also describes the logical connections to similar initiatives at European or global level.

This deliverable also identifies and describes the potential solutions and approach to support trust interoperability among IoT applications as requested in the WP4 description. Various solutions are possible, with different advantages and disadvantages.
<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
</table>


<table>
<thead>
<tr>
<th>Reference</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>(CISCO 2016b)</td>
<td>Achieve Cyber Security with the Help of Common Criteria Certification.</td>
</tr>
<tr>
<td></td>
<td>Official website. URL: <a href="http://www.isc2.org/cissp/default.aspx">http://www.isc2.org/cissp/default.aspx</a></td>
</tr>
<tr>
<td>(Coutant 2016)</td>
<td>Antoine Coutant. French Scheme CSPN to CC evaluation</td>
</tr>
<tr>
<td>(CRISC 2015)</td>
<td>CRISC - Certified in Risk and Information Systems Control.</td>
</tr>
<tr>
<td>(Dickson 2016)</td>
<td>Machine learning will be key to securing IoT in smart homes.</td>
</tr>
<tr>
<td>(ECORYS 2011)</td>
<td>Security Regulation, Conformity Assessment &amp; Certification</td>
</tr>
<tr>
<td></td>
<td>Final Report – Volume I: Main Report</td>
</tr>
<tr>
<td>(Elmiligi 2016)</td>
<td>Haytham Elmiligi, Fayez Gebali, M. Watheq El-Kharashi, Multi-dimensional analysis of embedded systems security, Microprocessors and Microsystems, Volume 41, March 2016,</td>
</tr>
<tr>
<td>Author/Source</td>
<td>Title/Details</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
</tr>
<tr>
<td>ETSI 2010</td>
<td>ETSI EN 302 665, Intelligent Transport Systems (ITS); Communications Architecture <a href="http://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf">Link</a></td>
</tr>
</tbody>
</table>
on the market of radio equipment and repealing Directive 1999/5/EC


| (Gubbi 2013) |

| (Hearn 2004) |

| (Hernández-Ramos 2015) |

| (IAPP 2016) |

| (ISASecure 2016) |

| (ISO 15408) |

| (ISO 16949) |
| ISO/TS 16949 Quality management standard for suppliers to the automotive sector |

| (ITSEC 1991) |

<p>| (Jackson 2007) |</p>
<table>
<thead>
<tr>
<th>Source</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(NIST 2016)</em></td>
<td>National Voluntary Laboratory Accreditation Program (NVLAP). Accreditation vs. Certification.</td>
</tr>
</tbody>
</table>
| (Salter 2011) | Common&Criteria & Reforms
http://www.sogis.org/ |
<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
</table>
| (TRUSTe 2016) | TRUSTe Privacy Certification Standards  
https://www.truste.com/privacy-certification-standards/  
| (UL 2016) | UL product testing and evaluation.  