EUROPEAN
COMMISSION

Brussels, 13.9.2017
SWD(2017) 500 final

PART 6/6

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')

{COM(2017) 477 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

Annex 8:

JRC Analysis and recommendations for a European certification and labelling framework for cybersecurity in Europe

JRC SCIENCE FOR POLICY REPORT

Analysis and recommendations for a European certification and labelling framework for cybersecurity in Europe

Gianmarco Baldini, Georgios Giannopoulos, Alessandro Lazari

2017

This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

Contact information
Name: Gianmarco Baldini
Address: Via Enrico Fermi 2749
Email: gianmarco.baldini@jrc.ec.europa.eu
Tel. : +39 0332 786618

JRC Science Hub
https://ec.europa.eu/jrc

JRC 105757

Luxembourg: Publications Office of the European Union, 2017

How to cite this report: Gianmarco Baldini et al., Analysis and recommendations for a European certification and labelling framework for cybersecurity in Europe, JRC 105757, 2017

Table of contents

Executive Summary 3
1 Introduction 5
2 Definitions 9
3 Existing certification schemes 11
3.1 International certification schemes 11
3.1.1 Common Criteria 11
3.1.2 The ISASecure Certification Programme 13
3.1.3 Information Technology Security Evaluation Criteria (ITSEC) 14
3.1.4 Federal Information Processing Standards FIPS-140 15
3.2 National Certification schemes 16
3.2.1 French security certification scheme 16
3.2.2 German security certification scheme 16
3.2.3 UK certification scheme 17
3.3 Other initiatives 18
3.3.1 Industrial Automation and Control Systems (IACS) 18
3.3.2 Common Criteria Recognition Arrangement (CCRA) 21
3.3.3 SOG-IS 21
3.3.4 UL 2900 certification. 22
3.3.5 Secure Change. 22
3.3.6 EN50128. 22
3.3.7 IEC61508 23
3.3.8 ISO 27001/27002 23
4 Analysis of the existing certification schemes 24
4.1 Issues and challenges 24
4.2 Domains applicability 27
4.2.1 Specific aspects of the energy sector 27
4.2.2 Specific aspects of the automotive sector 28
5 A way forward for a European certification scheme 31
5.1 Drivers for a new European certification scheme 31
5.2 Key elements of the new European security certification scheme 32
5.3 Labelling 35
5.4 Security and Privacy certification 36
5.5 Accreditation and testing laboratories 38
5.6 Main roles 39
5.7 Functional Architecture 40
5.8 Trusted applications 40

5.9 Market surveillance and monitoring 41
5.10 Model based testing (MBT) 42
5.11 Inherent risks and uncertainties 44
5.11.1 Obstacles to implementation 44
5.11.2 Potential negative effects 44
5.12 Recommendations 45
5.13 Policy Options 46
6 Conclusions 47
References 48
List of abbreviations 54
List of figures 56
List of tables 57
Annex: Report on the meeting of the experts on the 6th of December 2016 58
A.1. Background 58
A.2. Participants 58
A.3. Agenda of the meeting 59
A.4. Presentations and discussions 60
Sergio Lomban: The view from the European Cyber Security Organisation of cPPP 60
Arthur van der Wees (Arthur Legal) 62
Kai Rannenberg (Goethe University Frankfurt) 62
Paul Theron (Thales) 64
Philippe Cousin (Eglobalmark), Bruno Legeard (Université de Franche-Comté): ARMOUR project for security certification in IoT and Model Based Testing 65
Eireann Leverett of IOActive 66
A.5. Discussion 68
A.6. Conclusions of the meeting 71

Document History

Version	Date	Comments	Modified Pages
0.1	04/07/16	First draft	Initial version
0.2	27/09/16	Second version	Updated sections 4,5,6.4 and 6.10 after phoneCall on 28/09/2016.
0.3	01/10/16	Third version	Updated section on privacy
0.4	15/10/16	Fourth version	Minor Comments
0.5	21/10/16	Fifth Version	Added considerations for the automotive sector.
0.6	22/01/2017	Sixth version	Added report of the meeting on the 6th of December 2016
0.7	23/01/17	Seventh version	Added section on market monitoring.
0.8	31/01/17	Final version for internal review	Proof-read and other small checks
1.0	13/02/17	Final version	Changes after internal review.

Foreword

This report has been prepared in the context of the Administrative Arrangement Id 34294 between the JRC and DG CNECT to investigate and propose recommendations for the establishment of a European ICT security certification framework and to assess the feasibility of a European cybersecurity labelling framework. The report has been prepared on the basis of inputs received from security experts, Senior Officials Group Information System Security (SOG-IS) and DG CNECT H.1 - Cybersecurity and Digital Privacy.

Acknowledgements

We acknowledge the valuable input of DG CNECT H.1 colleagues Pierre Chastanet , Aristotelis Tzafalias and Domenico Ferrara, the colleagues of DG JRC E.3 Jean Pierre Nordvik, Igor Nai Fovino, Laurent Beslay and Ignacio Sanchez, the representatives of SOG-IS, ESCO-cPPP and AIOTI.

Executive Summary

Security certifications such as ITSEC and Common Criteria are often used to certify products in several domains such as in the case of Intelligent Transport Systems or SCADA. An example of the potential process can be found in the Cooperative-ITS domain where the certification and labelling process for C-ITS communication systems and ITS platforms is a key element to support the safety of the users. Similarly, information security management certifications such as ISO 27001 are often used to certify business processes and are also widely deployed in the industry.

Although these certification schemes are deemed as appropriate in certain areas, they are often perceived as too complex and resources consuming by the industry specially when applied to SMEs, which do not have the needed resources to implement such schemes.

In the context of the Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (COM (2016) 410), this report analyses the current state of art on the security certification processes at international and national level, and provides recommendations and policy options to support the establishment of an European security certification and labelling framework. The report identifies the key issues of the security certification processes to be addressed and proposes and European wide framework for security certification and compliance that can be effective in the delivery of trust, whilst at the same time reduces the burden typically introduced by other certification schemes. The key elements of this European framework are identified and described. Finally, the report provides recommendations for the design and deployment of a European security certification framework.

The recommendations provided in this report include the following:

1. A European security certification scheme should be set-up to overcome the national differences.
2. The basis for the new European security certification scheme shall be based on the Common Criteria.
3. A process to define harmonized protection profiles for specific domains should be put in place with the collaboration of existing organizations like SOG-IS or agreements like CCRA.
4. The definition of harmonized protection profiles is the basis for the definition of a labelling scheme to support the comparability and visibility of the security certification for end-users.
5. Security and privacy requirements should be validated in the same certification process and with the same harmonized protection profiles.
6. A process to create accredited security testing centres should be defined. The experience from the Horizon 2020 Future Internet Research & Experimentation (FIRE) could be useful at least for the IoT related products.
7. A post certification framework to support the lifecycle of products and to mitigate gaps in the security certification process and execution should be investigated and deployed.
8. The application of testing models and automated testing suites should be investigated in security certification to improve the efficiency of the security certification process and to address the issue of re-certification after product changes.

This study has been done taking in considerations other existing initiatives at European and national level in security certification and the current wider European regulatory

framework for conformity and compliance of products. Various meetings have been organized with SOG-IS and security experts in 2016, which are reported in DG JRC progress report JRC105854. A specific meeting was organized on the 6th of December 2016 with security experts to discuss together the main elements of the security certification framework and receive feedback on the priorities or feasibility of the proposed elements. A report of the meeting is provided in the Appendix.

Beyond security, the report does also take in consideration the certification of product against privacy requirements, especially in the prospect of the new Data Protection Regulation. We consider security and privacy closely related because security mechanisms can and should also be used for privacy protection (e.g., data confidentiality).

As preliminary set of policy options are described at the end of this report in section **Error! Reference source not found.** and they are briefly summarized here:

a) Encouraging and supporting the certification scheme. This option envisages the Commission using various soft measures to stimulate and encourage the adoption of security certification in Europe.
b) Definition of harmonized standards and protection profiles at European level. This option envisages the setting up of organizations and entities or the empowering of existing entities like SOG-IS and ETSI/CEN/CENELEC to define sets of harmonized protection profiles, without enforcing on the manufacturers binding measures.
c) Full regulation. This option envisages a full regulatory approach to secure certification for specific domains or applications.

1 Introduction

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 report, 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. Further details on this aspect are described in

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 (even if we show in the subsequent sections of this report that the commercial environment has seen an increase of security threats for a number of reasons). 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 3.1.1; 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) and section 3.

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 4.

In recent time, 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 the subsequent sections of the report.

This report provides a state of art on certification and labelling in different domains analyses and proposes more lightweight initiatives in the field of cybersecurity certification and compliance that can be effective in the delivery of trust whilst at the same time reduce the burden typically introduced by other certification schemes. In this context, lightweight does not mean that the security objectives should be addressed with minor attention but that some specific aspects of the security certification should be made more efficient.

To support the goal of a European certification and labelling scheme, two other aspects will be taken in consideration in this report:

1) the creation of a European networks of accredited certification centres, to support the certification scheme proposed in the report.
2) Exploitation of the existing conformity assessment processes for European products in general, where a regulatory framework has already been defined or it is being defined (EU 2008), the new Radio Equipment Directive (EU 2014) and the "Blue Guide" on the implementation of on the implementation of EU product rules 2016 (EU 2016)

2 Definitions

Accreditation	Accreditation shall mean an attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity. (EU 2008)
Certification	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. (NIST 2010)
CE marking	'CE marking' shall mean a marking by which the manufacturer indicates that the product is in conformity with the applicable requirements set out in Community harmonisation legislation providing for its affixing (EU 2008)
Compliance Assessment	Compliance assessment is an activity that helps to directly or indirectly identify the extent, to which a device or its constituent parts comply with the set of technical requirements, which must be validated to make the device operational. From an operational point of view, compliance assessment is an equipment authorization issued by a compliance assessment body based on representations and test data submitted by the applicant.
Conformance assessment	Conformance assessment means checking that products, materials, services, systems or people measure up to the specifications of a relevant standard.
Conformity assessment	Conformity assessment is the process carried out by the manufacturer of demonstrating whether specified requirements relating to a product have been fulfilled. (EU 2016)
Conformity / Compliance Testing	Conformance testing is the process used to determine whether a product or system complies with the requirements and/or functional specifications.
Declaration of Conformity	Declaration of Conformity is the conclusive step of a procedure where a responsible party makes measurements or takes other necessary steps to ensure that the equipment complies with the appropriate technical standards.
Manufacturer	Manufacturer shall mean any natural or legal person who manufactures a product or has a product designed or manufactured, and markets that product under his name or trademark. (EU 2008)
Protection Profile	A Protection Profile (PP) is a document used as part of the certification process according to ISO/IEC 15408 and the Common Criteria (CC)

Verification	Verification is a procedure where the manufacturer makes measurements or takes the necessary steps to ensure that the equipment complies with the appropriate technical standards.

3 Existing 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.

3.1 International certification schemes

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

3.1.1 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.

EAL level	Description
1	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.
2	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 "black box" testing, and evidence of a development search for obvious vulnerabilities.
3	Methodically Tested and Checked. The analysis is supported by "grey box" 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
4	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.
5	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.
6	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.
7	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 "white box" testing and complete independent confirmation of developer test results are required. Complexity of the design must be minimised.

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 4.1 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.

3.1.2 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.

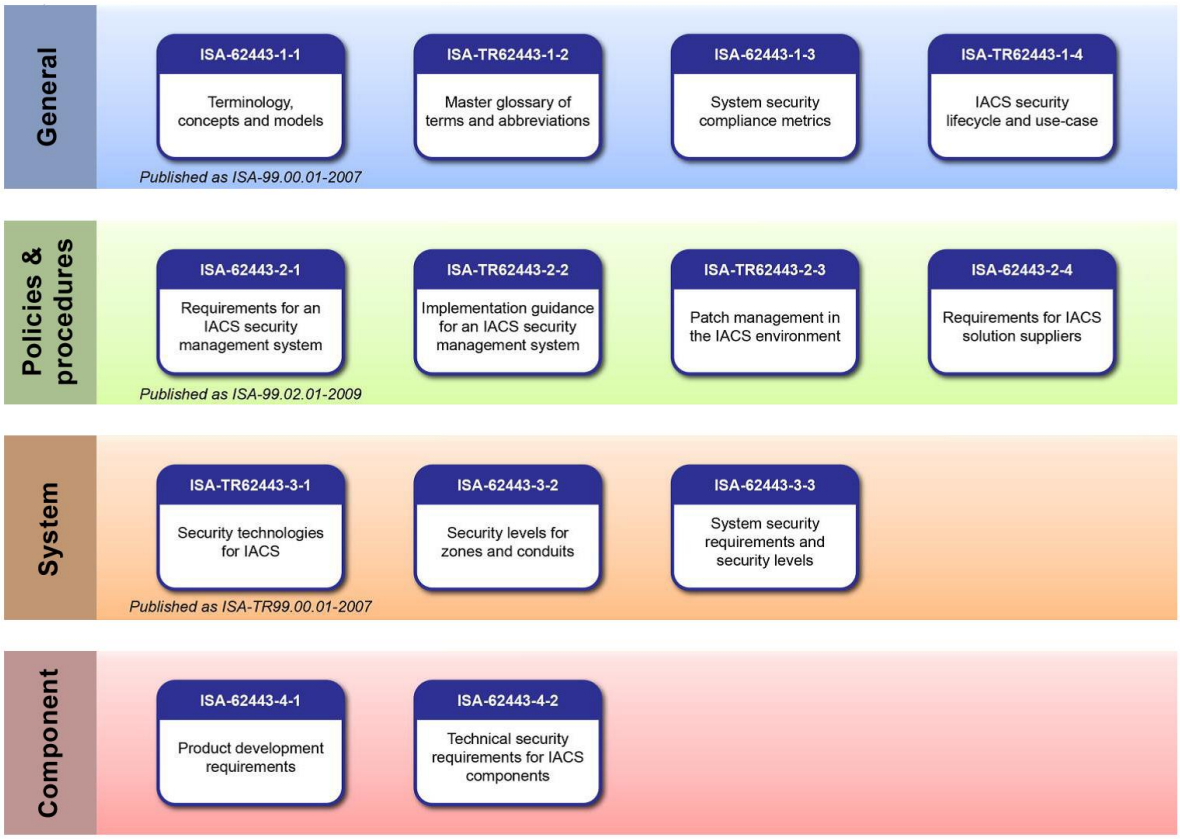

Figure 3 ISASecure certification scheme

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.

3.1.3 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 report.

3.1.4 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 report 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.

3.2 National Certification schemes

In this section, we will present the main European certification schemes at national levels. Only the main ones will be taken in consideration.

3.2.1 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 (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.
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.

3.2.2 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.

3.2.3 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.
- Accreditor, 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.

3.3 Other initiatives

Here we describe the other initiatives on security and safety certification, which are not addressed in the previous sections. These initiatives can be alternative or complementary to the certification processes described above. In addition, this section briefly describes security and safety certification schemes, which are not directly applicable to the subject matter of this report (cybersecurity), but they are historically relevant in their domains (e.g., rail, airplanes) and they can provide inputs to the analysis.

3.3.1 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'*.

[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.

[2] "Protecting Industrial Control Systems: Recommendations for Europe and Member States", Enisa, 2011. Available at the following link: https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states

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 huge 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 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's 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 asses 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);

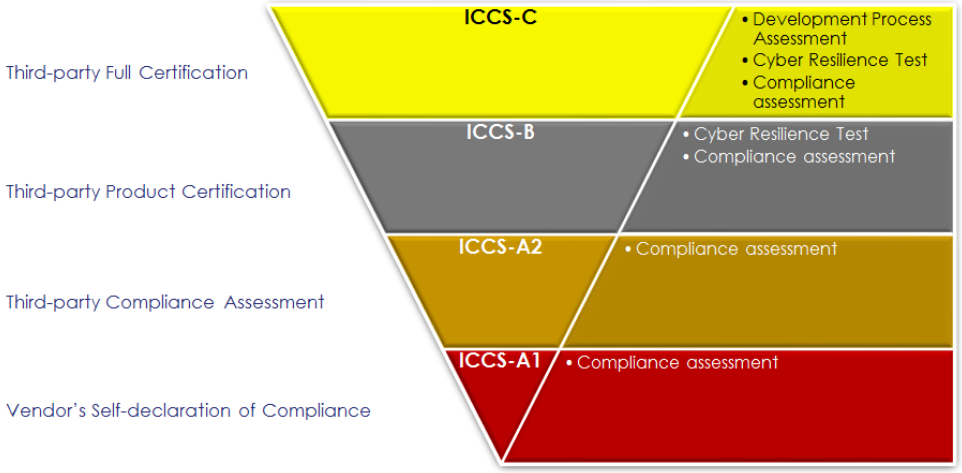

Figure 4 ICCF Compliance & Certification Levels.

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.

The ERNCIP's IACS Thematic Group is currently working on a second report (due in December 2016) that deepens the work in this field and should act as an orientation and feasibility study that provides:

- High level support to the implementation of the NIS directive;

- A framework to foster IACS components' cybersecurity certification;
- Four detailed schemes to motivate stakeholders to engage into certification at their own pace;
- Clear concepts and rules to help bridging with international schemes and containing certification's costs.

More in general, the ICCF aims at providing professionals within vendor, industry, laboratory and certification organisations with guidelines to make IACS components' cybersecurity certification happen more easily, at a controlled cost, and with recognition within and beyond European borders.

3.3.2 Common Criteria Recognition Arrangement (CCRA)

The objective of the CCRA 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.

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.

3.3.3 SOG-IS

The Senior Officials Group – Information Systems Security (SOG-IS) agreement was produced in response to the EU Council Decision of March 31st 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC) on common information technology security evaluation criteria.

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.

3.3.4 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).

3.3.5 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.

3.3.6 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 1 Security Integration Levels in coverage levels in EN50128 (from EN50128 standard)

	SIL 0	SIL 1	SIL 2	SIL 3	SIL 4
1. Statement Coverage	R	HR	HR	HR	HR
2. Branch Coverage	-	R	R	HR	HR
3. Composed conditions (MC/DC or MCC-Coverage)	-	R	R	HR	HR
4. Data Flow Analysis	-	R	R	HR	HR
5. Path Coverage	-	R	R	HR	HR

3.3.7 IEC61508

This standard covers functional safety and it is aimed at the electrotechnical 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.

3.3.8 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.

4 Analysis of the existing certification schemes

This is an important section of the report as it identifies the key challenges of the existing certification schemes and the need to create alternatives.

4.1 Issues and challenges

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 2 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 report does not directly endorse these statements even if they are used an in input to the analysis.

Table 2 Identified issues and criticisms of the Common Criteria approach

Identifier	Description	Source
1.	*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.*	(NCSA 2011)
2.	*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.*	(Jackson 2007)
3.	*no single set of criteria can be used to produce comparable and effective evaluations for a wide range of technologies*	(NCSA 2011)
4.	*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*	(ECORYS 2011)

	evaluation of software.	
5.	*Commonly used protection profiles often do not correspond to the functionality requirements actually required by users.*	(ECORYS 2011)
6.	*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 1 2 years, and, often, by the time the process is completed a new version of product is already delivered.*	(Kaluvuri 2014)
7.	*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)
8.	*Point in time certification. CC certificates 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)
9.	*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)
10.	*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)
11.	*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)
12.	*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*	(Hearn 2004)

	products contribute to overall system security when integrated into systems. Yet, without a system-level approach to security, and the metrics to 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)
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)
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)
16.	*Re-certification after changes being made in the product is not mandatory, but should be considered case by case*	(ENISA 2014)
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)
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)

From the analysis of the international security certification schemes, it is clear that the Common Criteria is endorsed by the main national bodies (France does also support Certification de Sécurité de Premier Niveau but the Common Criteria is also 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 2, 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 require the definition of a new process or a modification of the existing approach for Common Criteria.
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 items 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

In addition, we can identify the two following issues, which must be addressed in the definition of an European security certification framework in the current context:

8. *Joint certification of security and privacy*. With the introduction of the General Data Protection Regulation (GDPR) (see EU 2016b), it is preferable that both security and privacy certification is implemented in the same process.
9. *Accreditation and testing laboratories*. To support an European security certification framework, it is preferable that an harmonized accreditation process is set up for testing laboratories.

The recommendations of this report will focus on the actions, which can address the issues defined above.

4.2 Domains applicability

Security certification schemes were born in the defence domain, which is characterized by stringent security requirements, high costs of the equipment and very long lifecycles. Other domains do not share these characteristics and this is one of the main reason, why security certification and common criteria in particular has not been widely adopted in some domains (Anderson 2009) like the consumer market (e.g., smartphones).

On the other side, common criteria is most widely adopted security certification scheme and many products with limited capabilities like smartcards has been common criteria certified.

Indeed, the list of products and systems certified with Common Criteria is impressive and it is reported in (CCProd 2016). The list spans from smartcard and integrated circuits, database, detection systems, network and network-related devices and systems and other products used in many different domains.

As a consequence, it is not true that the Common Criteria cannot be applied a-priori to any domain, even if binding regulations in the specific domain apply and economic considerations can have an impact.

In the following paragraphs we describe the main aspects of two specific sectors: the energy sector and the cooperative intelligent transport system sector.

4.2.1 Specific aspects of the energy sector

While the ICT industry or the consumer mass market industry is entrepreneurial and freewheeling, with multiple overlapping and competing standards and fairly loose compliance, the electric power industry is different for safety reasons and for the huge scale of the infrastructures and the number of serviced users. Its engineers are meticulous about complying with every relevant standard because malfunctions can produce safety hazards and even kill people. In comparison to the automotive sector, which has similar safety issues, the engineers of the energy sector have to address very complex and interdependent infrastructures, where not all the dependencies (especially at the ICT level) are clearly identified. Some of the potential security threats are still not clearly understood and there is a growing body of research on security and privacy

aspects of the energy sector including its evolutions to the Smart Grid. The complexity and scale of future
power systems that incorporate smart-grid concepts will introduce many security challenges. Currently, a large utility communicates with thousands of devices to manage the electrical grid. Both the volume of data and the number of devices with which a utility communicates will likely increase by several orders of magnitude. With these larger networks, routine maintenance, managing trust, and monitoring for cyber intrusion become challenges. Certification of electronic components has already been largely adopted in the energy sector for safety reasons, but the introduction of more sophisticated ICT components will increase the need to integrate elements of security and privacy certification.

A more detailed study of the energy sector is provided in the report drafted by the Foundation for Information Policy Research (see reference FIPR 2016).

4.2.2 Specific aspects of the automotive sector

The automotive sector has quite strong requirements related to safety, while security aspects have not been substantially addressed because vehicles are basically protected by physical security. Until recently, cars were not connected to the outside word and the vehicle manufactures have full responsibility about safety and security. The Type approval and homologation processes had a very long history and the process is quite stable now, even if it can be quite expensive for vehicle manufacturers and it is fragmented, as there are different types approval requirements around the world. One example of this context is the internal vehicle network system mostly based on the CANBus set of standards. Not only this standard is quite old, but it is also not secure. This may change in the future because vehicles will be increasingly connected and new security threats may appear as demonstrated in recent incidents. There is an ongoing discussion on what type of security certification should be adopted for the new model of Cooperative ITS in Europe and Connected Vehicles in USA and it is not clear yet if the security certification of the wireless devices should be part of the type approval or not.

Cooperative Intelligent Transport Systems (C-ITS) is the term used to describe technology which allows vehicles to become connected to each other, and to the infrastructure and other parts of the transport network. In addition to what drivers can immediately see around them, and what vehicle sensors can detect, all parts of the transport system will increasingly be able to share information to improve decision making. Thus, this technology can improve road safety through avoiding collisions, but also assist in reducing congestion and improving traffic flows, and reduce environmental impacts. Once the basic technology is in place as a platform, an array of applications can be developed (from http://ec.europa.eu/transport/themes/its/c-its_en.htm).

The European Commission decided early 2014 to take a more prominent role in the deployment of connected driving, by setting up a C-ITS Deployment Platform. The Platform was conceived as a cooperative framework including national authorities, C-ITS stakeholders and the Commission, in view to develop a shared vision on the interoperable deployment of C-ITS in the EU. Hence, it was expected to provide policy recommendations for the development of a roadmap and a deployment strategy for C-ITS in the EU and identify potential solutions to some critical cross-cutting issues.

One of the key aspects is the compliance assessment process in C-ITS, whose main principles were defined in Working Group 5 of the C-ITS Deployment Platform and they have been published in (C-ITS 2016).

The following description of the compliance assessment process has been extracted from (C-ITS 2016) and the source documents, which generated (C-ITS 2016).

The compliance assessment process is used to certify C-ITS station for their deployment in the road transportation sector. A C-ITS station is roadside equipment or vehicle or

another mobile system, which can be connected using the 5.9 GHz Dedicated Short Range Communication system. Note that this is a simplification because the formal definition of an ITS station is provided in (ETSI 2010).

The overall architecture is shown in Figure 5.

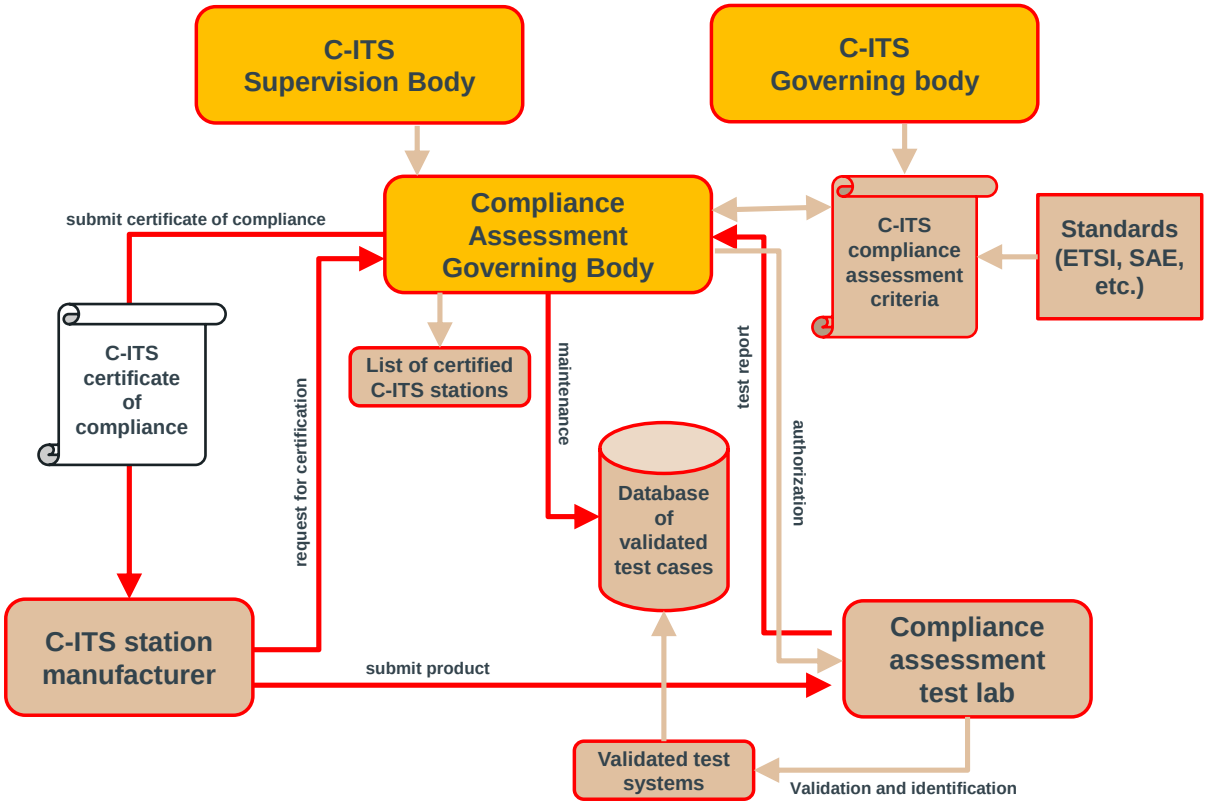

Figure 5 C-ITS European Compliance Assessment process

The main roles in the C-ITS European Compliance Assessment process are following.

The compliance assessment governing body is a centralized entity responsible for:

- Definition of compliance assessment criteria, which are compliant to and using the C-ITS Governing Body's input documents for operational and security requirements and the standards.
- handling of compliance assessment requests of C-ITS manufacturers
- definition of test scope for the compliance assessment (based on the C-ITS station type and functionality)
- definition of the minimum set of test criteria for the compliance assessment of every C-ITS station in order to be an interoperable node of the C-ITS Network
- submit certificate of compliance after successful C-ITS compliance assessment.
- maintenance of the list of certified C-ITS stations.
- authorization of ISO17025 accredited test labs (e.g. independent test labs)
  - based on frequent repetition of the accreditation in strict accordance on not yet defined certain criteria, but in accordance of the valid EU wide C-ITS Trust Model and the respective procedures:
  - nomination of qualified lab auditors
- maintenance of a database, which lists and stores validated test cases and validated test systems, which must be used for the execution of the test procedures for compliance assessment.

The Compliance Assessment Governing Body can be accredited according to the following standard:

- EN ISO/IEC 17065:2012 - Conformity assessment – Requirements for bodies certifying products, processes and services

The Compliance assessment test lab is responsible for

- the execution of test cases according to the C-ITS compliance assessment criteria.
- The testing will be performed:
  - by qualified persons
  - only on validated test systems
  - in a shielded lab environment
- validation of test cases on selected and validated test systems
- creating test reports and submission to the Compliance Assessment Governing Body

The Test Lab should be accredited according to the following standard:

- EN ISO/IEC 17025:2005 - General requirements for the competence of testing and calibration laboratories.

In addition, in order to build and operate the databases of C-ITS stations a Compliance Assessment Function is needed. To operate the database, the minimum requirements for conformance and performance needs to be established and maintained. This will typically consist of the following elements:

- Set of test cases per C-ITS station
- Compliance assessment Criteria for each type of C-ITS station (list of subset of test cases required to be passed for a given type of C-ITS station, and the minimum criteria for every validated C-ITS station in the network)
- Database of verified test cases and test implementations
- Rules for declaration of conformance.

5 A way forward for a European certification scheme

5.1 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 CCRA 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.

> Recommendation 1: A European security certification scheme should be set-up to overcome the national differences on security certification and support an european-wide cybersecurity market.

5.2 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 Issues and challenges 4.1 and address the drivers identified in section 5.1.

This new European security certification scheme can be also defined as lightweight certification scheme as it tries to streamline and make more efficient the security certification process for a wide range of ICT products. The term lightweight should not be understood as a weakening of the level of trust of the certified products but rather a more efficient way to certify the products according to different needs and different evaluation levels.

The key element 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 section 3, 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.
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 3.3.1 for a description of the IACS level.
3. *Labelling scheme*. A labelling scheme can be created to give a straightforward indication on the level of certified security of a product. The label concept is described more in detail in section 5.3, but the basic idea is to match labels to harmonized protection profiles at European level.
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 an European security certification process, some of the issues identified in section 4.1 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.
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 initiative could be exploited to support this network.
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 objective 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 provides, government, users, manufacturers) for the need of the definition of new harmonized protection profiles.

Recommendation 2: The basis for the new European security certification scheme shall be mainly based on the Common Criteria but new processes/standards should be defined for re-certification after product changes.

Recommendation 3: A process to define harmonized protection profiles for specific domains should be put in place with the collaboration of existing organizations like SOG-IS or agreements like CCRA.

These elements can address the issues of the existing certification schemes identified in section 4.1 as described in the following table:

Table 3 Key elements of the new European security certification scheme against the issues identified in section 3.4.1.

Key elements	**Issues**	**Comments**

A common European security certification scheme and the accompanying standard.	Mutual Recognition	By creating a common European security certification scheme, mutual recognition is ensured.
Certification scheme based on different certification levels	Certification costs	By adopting different levels of certification, the manufacturers can choose the most cost-effective security certification scheme for their products.
Labelling scheme	Comparability and visibility of the certification Security and trust coverage	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.
Harmonized protection profiles	• Mutual Recognition • Comparability and visibility of the certification	Harmonized protection profiles can support both mutual recognition and the labelling scheme to support the Comparability and visibility of the certification.
Evolution of Common Criteria	Re-certification and patching	The Common criteria process should be enhanced to address in a more efficient way the re-certification of an already certified product.
Accredited European security certification centres	Mutual Recognition	Accredited European security certification centres are a key element to guarantee an harmonized security certification process.
European Governing board	Mutual Recognition Non applicability to specific products and systems	The board will ensure European harmonization of the security certification process to support mutual recognition. The board will also address gaps and requests from stakeholder to mitigate the risk of non-applicability to specific products and systems.

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 centres

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.

A preliminary pictorial description on how the different key elements of the European security certification scheme are linked is provided in Figure 6.

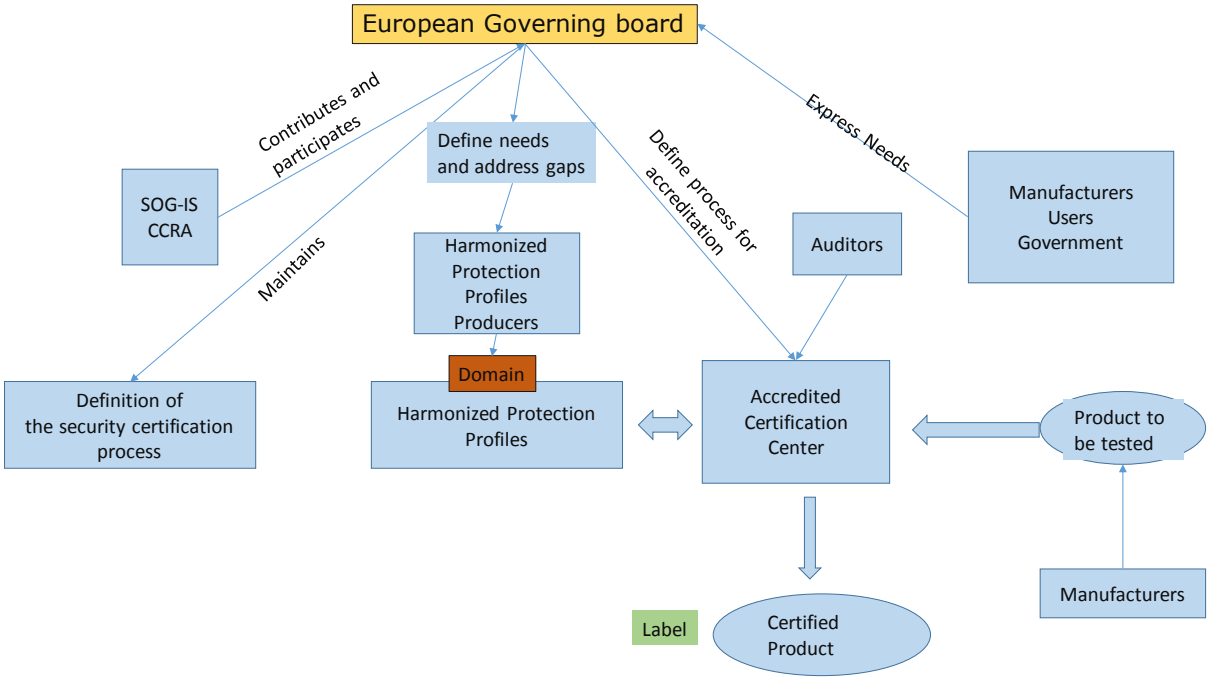

Figure 6 Overall scheme of the proposed European Security certification scheme

5.3 Labelling

The concept of applying a label on a product after a successful security certification is not new, as the EAL certificates from common criteria, the IACS (ERNCIP 2014), the four levels of FIPS can all be related to a labelling scheme, which gives an indication on the level of security protection or trust of a system.

The critical task is how to associate the labels in a harmonized way across different certification schemes, protection profiles and so on.

In France, the ANSSI has also defined a label system for trusted products and service providers. Currently, ANSSI recognises and issues two main types of labels. These labels are used for:

- certifying products
- qualifying products and services

The labelling concept could be extended to cover not only the traditional levels of Common Criteria (EAL), but to address specific security functions, which can be linked to specific protection profiles. For example, labels could be defined for specific security properties like confidentiality, integrity and authentication or for a specific Security Target (ST), which is defined in the related protection profile.

We can define different dimensions for which the label can be defined:

1. Level of assurance. This is the equivalent of the EAL in Common Criteria. We note that EAL level does not measure the security of the system itself, it simply states at what level the system was tested.

2. Protection profile for a specific domain (energy, road transportation and so on). Each protection profile can be associated to a specific level of assurance (dimension 1). Each domain has its own specific features and configuration environment, which must take in consideration for the security certification and deployment. For example, the security certification of a crypto-module for the road transportation may not be valid for the energy sector. This is why, the label must have a separate dimension to identify the domain.
3. To define how the certification was achieved: self-certification, third-party compliance assessment and so on how it is defined for IACS in section 3.3.1.

Figure 7 describes the label scheme and its dimensions.

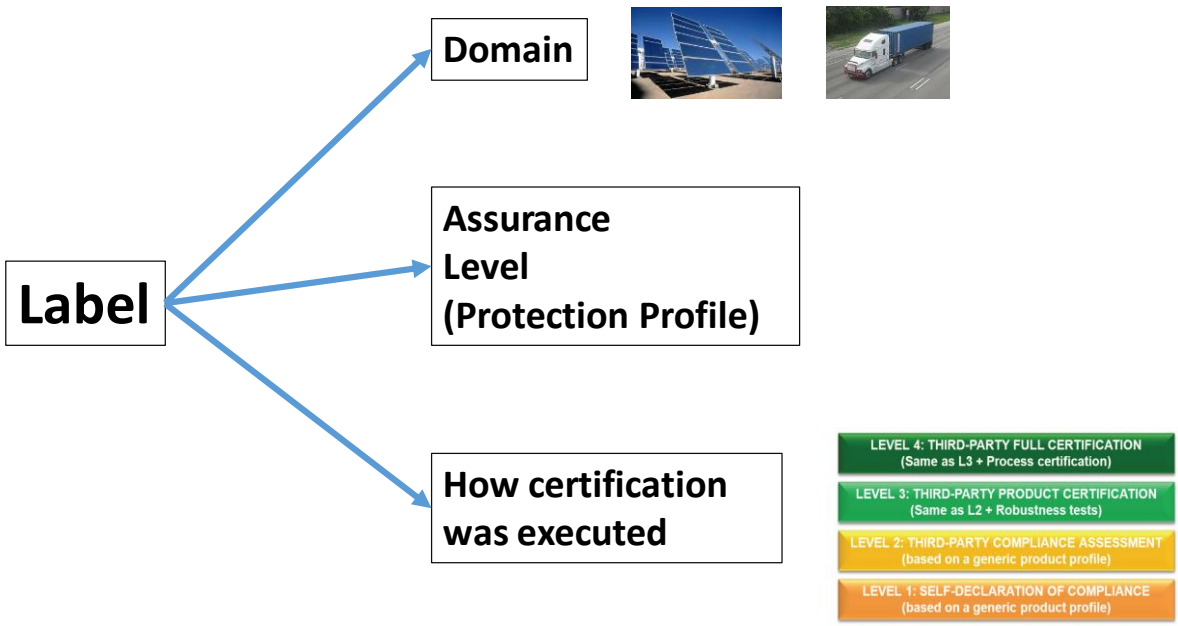

Figure 7 Label scheme and its dimensions

Recommendation 4: The definition of harmonized protection profiles is the basis for the definition of a labelling scheme to support the comparability and visibility of the security certification for end-users. A labelling scheme at European level should be put in place.

5.4 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 described in section 5. 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 report:

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 report) initiatives to define harmonization actions like SOG-IS in the privacy area apart from EuroPriSe.
3) At the time of writing this report, 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 report 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 8.

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.

Recommendation 5: Security and privacy requirements should be validated in the same certification process and within the same harmonized protection profiles.

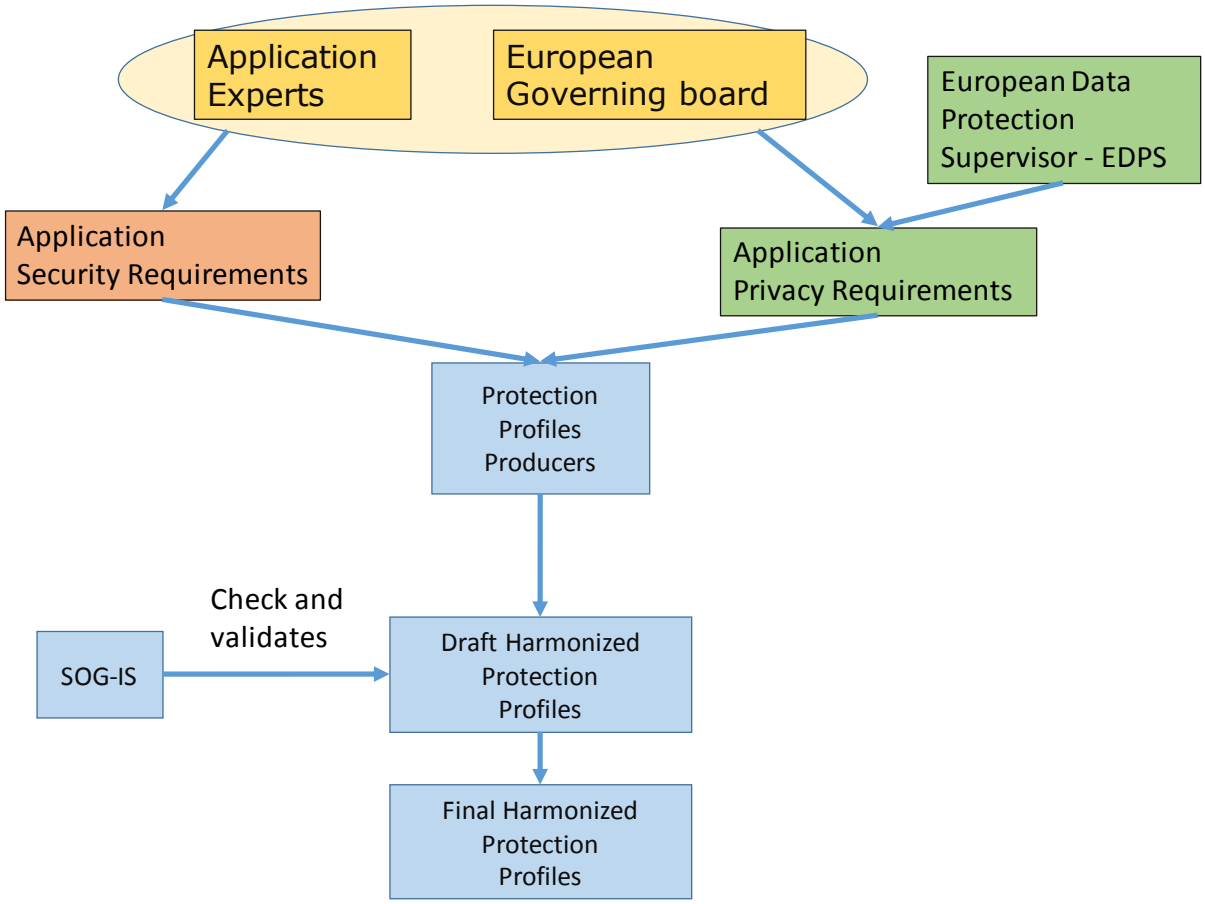

Figure 8 Security and Privacy flows

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 seas is focused on the incorporation of the *EU data protection requirements into an existing EU certification scheme*, which is the same approach identified here.

5.5 Accreditation and testing laboratories

Testing laboratories are an important element of security certification. The goal of this section is to describe the role of the testing laboratories in security certification.

The Testing laboratory is where the tests needed to achieve security certification of a product or a system are actually performed. To perform such tests and provide a certificate of compliance of the product, the testing laboratory itself must be itself evaluated. This process is called accreditation and it is defined in (NIST 2016) as:

"Accreditation is used to verify that laboratories have an appropriate quality management system and can properly perform certain test methods (e.g., ANSI, ASTM, and ISO test methods) and calibration parameters according to their scopes of accreditation".

One of the most common standard used to perform accreditation of testing laboratories is the ISO/IEC 17025 standard.

ISO/IEC 17025:2005 is a standard, which defines the requirements for the capabilities to carry out tests and/or calibrations. It covers testing and calibration performed using standard methods, non-standard methods, and laboratory-developed methods.

It is applicable to all organizations performing tests and/or calibrations. These include, for example, first-, second- and third-party laboratories, and laboratories where testing and/or calibration forms part of inspection and product certification.

In USA, the National Voluntary Laboratory Accreditation Program (NVLAP) accredits testing laboratories to meet the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme requirements and conduct IT security evaluations for conformance to the Common Criteria.

In Europe, a number of firms have been certified as Commercial Licensed Evaluation Facilities (CLEFs) under the Common Criteria in UK, as Centres d'Evaluation de la Sécurité des Technologies de l'Information (CESTI) in France and IT Security Evaluation Facility (ITSEF) in Germany.

The accreditation process in the world and especially in Europe is well deployed and based on a well-defined standard (ISO/IEC 17025:2005). Potential improvements of the accreditation process can be more focused on the way the tests are conducted in the lab. Most of the test suites and the test bed capabilities are focused on rule-based or standard-based compliance while many security failures are due to security attacks. Testing labs could become more competent and be accredited for testing of adversarial thinking by hackers. This improvement obviously requires additional capabilities and cost, so it cannot be applied to all the existing accredited labs.

Two levels of accredited labs could be foreseen, with the first level based on conventional accreditation and the second level based on the previous recommendation.

Another potential improvement of the accreditation process is that accreditation can be often focused either on safety (e.g., mechanical incidents in railways) or security (e.g., cybersecurity threat). While, in the past, this separated approach could be acceptable, the on-going evolution of ICT and its growing role in critical infrastructures or cyber-physical systems, will probably require an accreditation process, which combines safety and security.

Recommendation 6: A process to create accredited security testing centres should be defined. While existing processes can be used, they should be reviewed according to the new security certification framework.

5.6 Main roles

Here we describe the possible roles for a European certification scheme. Note that some of the roles have been already identified in the previous section 5.2.

- 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. The EGB is also responsible to define the labels in different domains.
- Accredited certification centre. This is the certification centre, which performs the test execution on the basis of the pre-defined harmonized protection profile.
- 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 would 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.

The functions of the different roles can change depending on the policy options, which are described in section **Error! Reference source not found.**.

5.7 Functional Architecture

The definition of the functional architecture is still premature at this stage. The objective of this section is to describe in detail figure 6 and also to describe the main information flows among the main elements of the security certifications.

This can be done only when all the other elements of the framework have been evaluated and assessed.

5.8 Trusted applications

This section is used to define how the security certification of products and devices can be used to enhance the trust of application or system. The main concept is that certified devices and products with a specific label can be used to build a trusted application or systems. Note that this concept has been criticized in (ERNCIP 2014) and other sources, because some security properties (authentication) may not be composed. For example, an application, which has been built only with security products, which are security certified for a specific level (and they have an appropriate label) does not automatically imply that the application will be successfully certified for that level, even if they are in the same domain. This topic is still discussed. The key issue is that the formal

modelling of a system and its components from a security certification point of view is a complex task. The Horizon 2020 ARMOUR project (www.armour-project.eu) has the objective to answer this question and define a formal framework for the security certification of products and systems , which links the formal definition of the system, the protection profile s, the set of tests to be executed for the certification and finally the labelling process.

5.9 Market surveillance and monitoring

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.

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 2016b) 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.

Recommendation 7: A post certification framework to support the lifecycle of products and to mitigate gaps in the security certification process and execution should be investigated and deployed.

5.10 Model based testing (MBT)

This section has the objective 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.

The Horizon 2020 ARMOUR project investigates 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 JRC is actively participating to this project.

The following text and figures are extracted from the deliverables of ARMOUR (deliverable D2.2). Even if the ARMOUR project is still on progress (it started in February 2016), some results are already useful for the objective of this report and they are provided here.

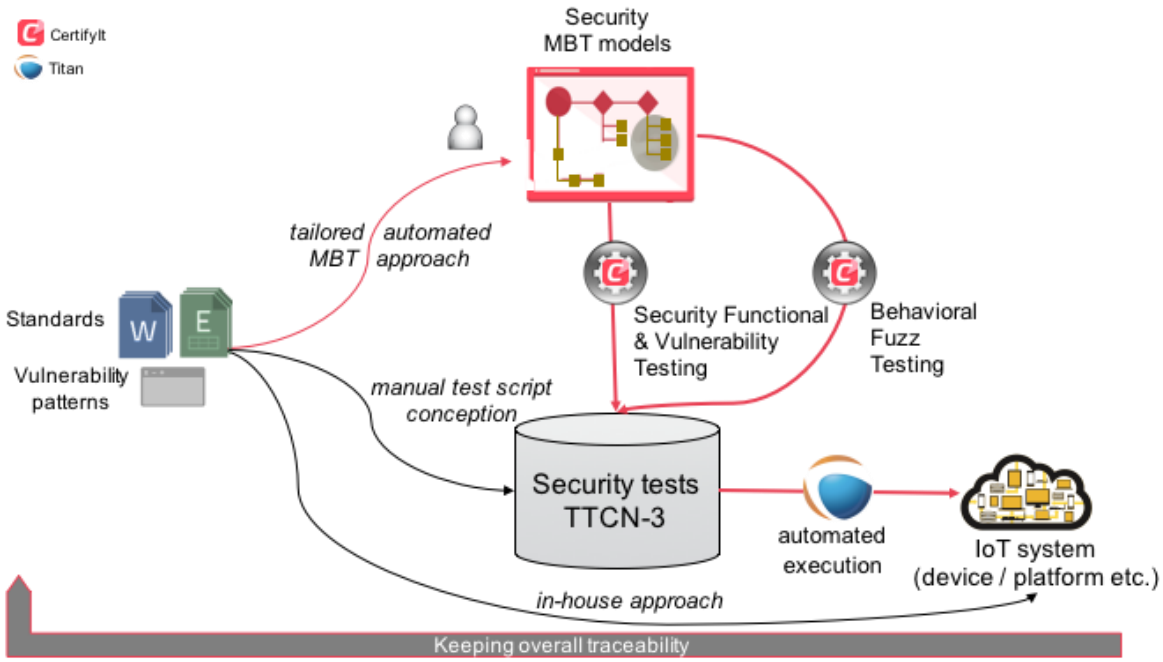

Figure 9 ARMOUR MBT Security Testing Framework

The overall framework is decribed in Figure 9. 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 standars 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 support 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.
3. MBT and TTCN suites can be linked directly to the labelling concept described in the other sections of this report.

Recommendation 8: The application of testing models and automated testing suites should be investigated in security certification to improve the efficiency of the security certification process and to address the issue of re-certification after product changes

5.11 Inherent risks and uncertainties

The aim of this section is to discuss the potential risks and uncertainties of the proposed certification framework and identifies the potential show stoppers.

5.11.1 Obstacles to implementation

The European certification scheme described in section 5 will require the definition of various organization bodies and new processes, which will be complex and time consuming to define. Even if existing bodies (accredited labs, SOG-IS) could be key elements, which are already present today, there is a significant amount of work to be done before such a framework (or a similar framework) could be created. In addition, economic aspects could have an impact on the definition of the framework and there are trade-offs (described in this report) between a voluntary and a mandatory (e.g., regulation) approach.

The following key issues are identified:

1. On which regulatory framework, the new security certification framework will be created ? Each domain has already regulatory frameworks in place (road transportation, healthcare), which are going to impose specific requirements, procedures and organizational entities. The question is how these organization entities will interact with the elements defined in section 5.6.
2. There could be considerable resistance from the manufacturers community if security certification is imposed on a non-voluntary basis.
3. The maintenance of the protection profiles, labels and processes could be quite time consuming and complex for the involved organizations.
4. New interfaces must be defined among old organizations and new organizations for the definition of the European security certification framework.
5. Security certification of applications and services can be significantly more complex than security certification of products. While, a clear definition of services and applications is missing in this context, there is the risk that security certification may be difficult to achieve for large and complex ICT applications.

5.11.2 Potential negative effects

While an European security certification framework can provide the benefits described in this report, we should also be careful to introduce negative impacts. A mandatory security certification can introduce additional costs on the manufacturer and the citizen. While some types of products would require secure certification because of safety reasons (healthcare, road transportation) other products may be based on a voluntary basis approach.

From an economic point of view, there is also the risk to introduce market distortion because large/midsize companies would be able to invest more money on the security certification process, while small companies could be excluded by some markets.

The dynamicity of specific domains or technologies (e.g., IoT) introduces the issue of the staticity of security certification, which is already described in the report. This means that if a product is submitted to frequent changes, the security certification will be not worth the effort involved in the initial phases

5.12 Recommendations

In this section, we list the main recommendations identified in the previous sections.

1) A European security certification scheme should be set-up to overcome the national differences on security certification and support an european-wide cybersecurity market. The key elements of the European certification scheme can include the ones proposed in section 5 or additional ones to be defined.
2) The basis for the new European security certification scheme shall be mainly based on the Common Criteria but the issues identified in section 4.1 should be addressed with the definition of new processes. In particular, for the re-certification after product changes.
3) A process to define harmonized protection profiles for specific domains should be put in place with the collaboration of existing organizations like SOG-IS or agreements like CCRA.
4) The definition of harmonized protection profiles is the basis for the definition of a labelling scheme to support the comparability and visibility of the security certification for end-users. A labelling scheme should be put in place. Labels can be defined on the basis of different dimensions as described in section 5.3.
5) Security and privacy requirements should be validated in the same certification process and with the same harmonized protection profiles.
6) A process to create accredited security testing centres should be defined. While existing processes can be used, they should be reviewed according to the new security certification framework.
7) A post certification framework to support the lifecycle of products and to mitigate gaps in the security certification process and execution should be investigated and deployed.
8) The application of testing models and automated testing suites should be investigated in security certification to improve the efficiency of the security certification process and to address the issue of re-certification after product changes.

5.13 Policy Options

This section has the objective to identify the main potential policy options for the implementation of the certification framework.

The three main policy options are possible:

1) **Encouraging and supporting the certification scheme**. This option envisages the Commission using various soft measures to stimulate and encourage the adoption of security certification in Europe. The aim is to encourage secure certification through non-binding measures, which can include the identification of objectives and the definition of general guidelines. In this policy option, security certification is still on a voluntary basis. There is no harmonization among domains for security certification but actions are put in place to support harmonization of the security certification processes. Labels are defined on a voluntary basis.

2) **Definition of harmonized standards and protection profiles at European level**. This option envisages the setting up of organizations and entities or the empowering of existing entities like SOG-IS and ETSI/CEN/CENELEC to define sets of harmonized protection profiles, without enforcing on the manufacturers binding measures. In other words, the EC could financially support the definition of the harmonized protection profiles, but there will not be an enforcing and binding regulation in place. Harmonized profiles across Europe for different domains are defined. Accredited test beds are identified to perform security certification with the same processes across Europe. Labels are identified and defined but only for partial sets of products (e.g., used in the government procurement).

3) **Full regulation**. This option envisages a full regulatory approach to secure certification for specific domains or applications. This option covers a scenario where decision-makers and other stakeholders intentionally choose to construct a fully-regulated scheme that will leave no space for derogations, disharmonised approaches or divergent implementations at the Member State or end user level. Although this could take place under other policy options too (e.g., specific policies in the energy or transportation domain), in essence this policy option refers to the intention of decision-makers not to leave the final outcome open to circumstances and the conditions in the market or the Member State level. In this option, harmonized profiles across Europe for different domains are defined and they are closely associated to labels. Labels are used by different types of users and consumers.

6 Conclusions

This preliminary report has investigated and identified key issues of existing security certification schemes (e.g., Common Criteria) on the basis of a literature review and input from security experts. In particular, the report has taken in consideration the input from previous reports and publications on the same topic (ESCO-cPPP, AIOTI, IACS) and direct feedback from security experts and security organizations like SOG-IS and ENISA. To address these issues, the report proposes a new European security certification framework, which is able to mitigate the identified issues and supports an European wide cybersecurity market. The key elements of this European security certification framework are based on existing entities (e.g., accredited test labs, SOG-IS) and standards (e.g., evolution of Common Criteria and CSPN) complemented by new processes and organizational structures. In particular, the report recommends the application of formal testing methods (e.g., Model Based Testing) and post-certification monitoring.

The preliminary concepts proposed in this report should be further assessed and evaluated with the directorates of the European Commission to evaluate the feasibility of the concepts in different domains (e.g., road transportation, energy), members of the industry community (ESCO-cPPP, AIOTI, IACS), member states SOG-IS and other stakeholders (ENISA).

References

(Anderson 2008)	Anderson, R., Böhme, R., Clayton, R., & Moore, T. (2008). Security economics and the internal market. Study commissioned by ENISA.
(Anderson 2009)	Anderson, R., & Fuloria, S. Certification and evaluation: A security economics perspective. In Emerging Technologies & Factory Automation, 2009. ETFA 2009. IEEE Conference on (pp. 1-7). IEEE. Sempteber 2009.
(ANSSI 2015)	ANSSI security certification http://www.ssi.gouv.fr/uploads/2014/10/certification_en.pdf. Last accessed 12/June/2016.
(Arstechnica 2016)	Underwriters Labs refuses to share new IoT cybersecurity standard http://arstechnica.com/security/2016/04/underwriters-labs-refuses-to-share-new-iot-cybersecurity-standard. Last accessed 12/June/2016.
(Beznosov 2004)	Beznosov, K., & Kruchten, P. (2004). Towards agile security assurance. In *Proceedings of the 2004 workshop on New security paradigms* (pp. 47-54). ACM.
(BSI 2012)	Technical information on the IT security certification of products, protection profiles and sites. BSI 7138. November 2012.
(CC 2008)	Common Criteria Protection Profile Firewall V2.0 https://www.commoncriteriaportal.org/files/ppfiles/FW%20PP-93-EN.pdf
(CC 2012)	Common Criteria Management Committee Vision Statement http://www.commoncriteriaportal.org/files/ccfiles/2012-09-001_Vision_statement_of_the_CC_and_the_CCRAv2.pdf. Last accessed 12/June/2016.
(CC 2014)	Collaborative Protection Profiles. The benefits of an evolved Common Criteria Implementation. September 2014. http://www.ccusersforum.org/library/wp/cPP_White_Paper.pdf. Last accessed June 2016.
(CC 2016)	Common Criteria v3.1. Release 4 Part 1: Introduction and general model at https://www.commoncriteriaportal.org/cc/. Last accessed 12/June/2016.
(CCProd 2016)	Common Criteria products https://www.commoncriteriaportal.org/products/ Last accessed 12/June/2016.
(CCSP 2015)	CCSP - Certified Cloud Security Professional. Official website. URL: https://www.isc2.org/ccsp/default.aspx
(CESG 2016)	UK ITsec Evaluation & Certification Scheme: UKSP01 - Description of the Scheme. https://www.cesg.gov.uk/documents/uk-itsec-

	evaluation-certification-scheme-uksp01-description-scheme. Last accessed 12/June/2016.
(CISA 2015)	CISA – Certified Information Systems Auditor. Official website. URL: http://www.isaca.org/certification/cisa-certified-information-systems-auditor/pages/default.aspx
(CISCO 2016)	Achieve Cyber Security with the Help of Common Criteria Certification. http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/cyber.pdf. Last accessed 12/June/2016.
(CISCO 2016b)	Securing the Internet of Things: A Proposed Framework http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html
(CISM 2015)	CISM - Certified Information Security Manager. Official website. URL: http://www.isaca.org/certification/cism-certified-information-security-manager/pages/default.aspx
(CISSP 2015)	CISSP - Certified Information Systems Security Professional . Official website. URL: https://www.isc2.org/cissp/default.aspx
(C-ITS 2016)	C-ITS Platform Final Report. http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf
(CRISC 2015)	CRISC - Certified in Risk and Information Systems Control. Official website. URL: http://www.isaca.org/certification/crisc-certified-in-risk-and-information-systems-control/pages/default.aspx
(Dickson 2016)	Machine learning will be key to securing IoT in smart homes. https://iotsecurityfoundation.org/machine-learning-will-be-key-to-securing-iot-in-smart-homes/. Last accessed January 2017.
(Dusart 2008)	Dusart, P., Sauveron, D., Tai-Hoon, K.: Some Limits of Common Criteria Certification. International Journal of Security and its Applications 2(4), 11–20 (2008)
(ECORYS 2011)	Security Regulation, Conformity Assessment & Certification Final Report – Volume I: Main Report Brussels October 2011. http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/security/pdf/secerca_final_report_volume_1_main_report_en.pdf. Last accessed 12/June/2016.
(Elmiligi 2016)	Haytham Elmiligi, Fayez Gebali, M. Watheq El-Kharashi, Multi-dimensional analysis of embedded systems security, Microprocessors and Microsystems, Volume 41, March 2016, Pages 29-36, ISSN 0141-9331, http://dx.doi.org/10.1016/j.micpro.2015.12.005. Last accessed 12/June/2016.

(ENISA 2014)	Minutes of the Joint EC/ENISA SOG-IS and ICT certification workshop. October 2014 ENISA. https://www.enisa.europa.eu/events/sog-is/minutes. Last accessed 6/June/2016.
(ERNCIP 2014)	Proposals from the ERNCIP Thematic Group, "Case Studies for the Cyber-security of Industrial Automation and Control Systems", for a European IACS Components Cyber-security Compliance and Certification Scheme https://erncip-project.jrc.ec.europa.eu/component/jdownloads/send/16-case-studies-for-industrial-automation-and-control-systems/60-proposals-from-the-erncip-thematic-group-case-studies-for-the-cyber-security-of-industrial-automation-and-control-systems-for-a-european-iacs-components-cyber-security-compliance-and-certification-scheme?option=com_jdownloads. Last accessed 12/June/2016.
(ETSI 2010)	ETSI EN 302 665, Intelligent Transport Systems (ITS); Communications Architecture http://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf
(EU 2008)	REGULATION (EC) No 765/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93
(EU 2013)	EU privacy seals project Inventory and analysis of privacy certification schemes. Rowena Rodrigues, David Barnard-Wills, David Wright. http://bookshop.europa.eu/en/eu-privacy-seals-project-pbLBNA26190/ ISBN: 978-92-79-33275-3
(EU 2014)	DIRECTIVE 2014/53/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC
(EU 2016)	COMMISSION NOTICE of 5.4.2016 The 'Blue Guide' on the implementation of EU product rules 2016. Brussels, 5.4.2016 C(2016) 1958 final
(EU 2016b)	General Data Protection Regulation. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

(FIPS 2002)	FIPS PUB 140-2 Security requirements for cryptographic modules. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf. Last accessed 12/June/2016.
(FPIR 2016)	Standardisation and Certification of Safety, Security and Privacy in the `Internet of Things'. Report produced by FPIR for the European Commission – DG JRC, JRC105840.
(GFC 2016)	Global Compliance assessment Forum (GCF). http://www.globalcertificationforum.org. Last accessed 12/June/2016.
(Hearn 2004)	J. Hearn, "Does the common criteria paradigm have a future?," in IEEE Security & Privacy, vol. 2, no. 1, pp. 64-65, Jan.-Feb. 2004.
(IAPP 2016)	Europe's privacy seal schemes gradually taking shape https://iapp.org/news/a/europes-privacy-seal-schemes-gradually-taking-shape/
(ISASecure 2016)	IEC 62443 CONFORMANCE CERTIFICATION Certifying Industrial Control System Devices and Systems http://www.isasecure.org/en-US/Certification. Last accessed 12/June/2016.
(ISO 15408)	ISO/IEC 15408. ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model.
(ISO 16949)	ISO/TS 16949 Quality management standard for suppliers to the automotive sector
(ITSEC 1991)	Information Technology Security Evaluation Criteria (ITSEC) version 1.2. 1991 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile. Last accessed 12/June/2016.
(Jackson 2007)	Under Attack https://gcn.com/articles/2007/08/10/under-attack.aspx. Last accessed 12/June/2016.
(Kaluvuri 2014)	"A Quantitative Analysis of Common Criteria Certification Practice" Kaluvuri, Samuel Paul, Bezzi, Michele, Roudier, Yves, Eckert, Claudia, Katsikas, Sokratis K., Pernul, Günther Trust, Privacy, and Security in Digital Business: 11th International Conference, TrustBus 2014, Munich, Germany, September 2-3, 2014. Proceedings Springer International Publishing
(Kaluvuri 2014)	Kaluvuri, Samuel Paul, Michele Bezzi, and Yves Roudier. "A Quantitative Analysis of Common Criteria Certification Practice." In Trust, Privacy, and Security in Digital Business, pp. 132-143.

	Springer International Publishing, 2014.
(Lipner 2015)	S. B. Lipner, "The Birth and Death of the Orange Book," in IEEE Annals of the History of Computing, vol. 37, no. 2, pp. 19-31, Apr.-June 2015.
(Murdoch 2012)	Murdoch, S. J., Bond, M., & Anderson, R. (2012). How certification systems fail: Lessons from the Ware report. IEEE Security & Privacy, 10(6), 40-44.
(NCSA 2011)	"Common Criteria Reforms: Better Security Products through Increased Cooperation with Industry", available at: http://www.niap-ccevs.org/cc_docs/CC_Community_Paper_10_Jan_2011.pdf. Last accessed 12/June/2016.
(NIST 2010)	NIST Special Publication 800-37. Guide for Applying the Risk Management Framework to Federal Information Systems. February 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf. Last accessed 12/June/2016. https://www.nist.gov/national-voluntary-laboratory-accreditation-program-nvlap/accreditation-vs-certification
(NIST 2016)	National Voluntary Laboratory Accreditation Program (NVLAP). Accreditation vs. Certification.
(Raschke 2014)	Raschke, W., Zilli, M., Baumgartner, P., Loinig, J., Steger, C., & Kreiner, C. (2014, August). Supporting evolving security models for an agile security evaluation. In Evolving Security and Privacy Requirements Engineering (ESPRE), 2014 IEEE 1st Workshop on (pp. 31-36). IEEE.
(RED 2014)	Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32014L0053 Last accessed 12/September/2016.
(SAAR 2008)	Saar Drimer, Steven J. Murdoch, and Ross Anderson. Thinking inside the box: system-level failures of tamper proofing. In IEEE Symposium on Security and Privacy (Oakland), pages 281–295, May 2008
(Salter 2011)	Common&Criteria & Reforms https://web.archive.org/web/20120417104556/http://www.niap-ccevs.org:80/cc_docs/CC_Community_Paper_10_Jan_2011.pdf

(Sauveron 2007)	D. Sauveron and P. Dusart, "Which Trust Can Be Expected of the Common Criteria Certification at End-User Level?," Future Generation Communication and Networking (FGCN 2007), Jeju, 2007, pp. 423-428.
(Sauveron 2007)	Sauveron, D., Dusart, P.: Which Trust Can Be Expected of the Common Criteria Certification at End-User Level: Future Generation Communication and Networking, 2, 423–428 (2007)
(SOGIS 2016)	Mutual Recognition Agreement Senior Officials Group Information Systems Security (SOG-IS) http://www.sogis.org/. Last accessed 12/June/2016.
(TRUSTe 2016)	TRUSTe Privacy Certification Standards https://www.truste.com/privacy-certification-standards/ Last accessed 12/September/2016.
(UL 2016)	UL product testing and evaluation. http://industries.ul.com/software-and-security/product-security-services/product-testing-and-validation. Last accessed 12/June/2016.
(Ware 1979)	Willis H. Ware. Security controls for computer systems: Report of defense science board task force on computer security. Report R-609-1, RAND Corporation, January 1970. Reissued October 1979.
(Yan 2014)	Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. Journal of network and computer applications, 42, 120-134.

List of abbreviations

ANSSI	French Network and Information Security Agency
CAC	Conformity Assessment and Certification
CB	Certification/Validation Body
CCRA	Common Criteria Recognition Arrangement
CESG	Communications-Electronics Security Group
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
C-ITS	Cooperative Intelligent Transportation Systems
CLEFs	Commercial Evaluation Facilities
COAs	Certificate Of Authenticity
CRISC	Certified in Risk and Information Systems Control
CSP	critical security parameters (CSP)
DPA	Differential Power Analysis
EAL	Evaluations Assurance Levels
EDPB	European Data Protection Board
ERNCIP	European Reference Network for Critical Infrastructure Protection
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
IACS	Industrial Automation and Control Systems
IACS	Industrial Automation and Control Systems
IC	Integrated Circuits
ICCS	IACS Compliance & Certification Schemes
IoT	Internet of Things

ISMS	Information Security Management System
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria
MBT	Model based testing
NVLAP	National Voluntary Laboratory Accreditation Program
OCL	Object Constraint Language
SIL	Security Integration Levels
SOGIS	Senior Officials Group – Information Systems Security
SPA	Simple Power Analysis
TOE	Target of Evaluation
TTCN	Testing and Test Control Notation

List of figures

Figure 1 Levels of products evaluation in the Orange book 6
Figure 2 Definition of EALs from Common Criteria extracted from (ECORYS 2011). 12
Figure 3 ISASecure certification scheme 14
Figure 4 ICCF Compliance & Certification Levels. 20
Figure 5 C-ITS European Compliance Assessment process 29
Figure 6 Overall scheme of the proposed European Security certification scheme 35
Figure 7 Label scheme and its dimensions 36
Figure 8 Security and Privacy flows.....38
Figure 9 ARMOUR MBT Security Testing Framework 43
Figure 1 Security certification presented by Prof Rannenberg.....63
Figure 2 Four levels of certification in IACS 64
Figure 3 Examples of the application of the testing concepts of ARMOUR project. 66

List of tables

Table 1 Security Integration Levels in coverage levels in EN50128 (from EN50128 standard) 23

Table 2 Identified issues and criticisms of the Common Criteria approach 24

Table 3 Key elements of the new European security certification scheme against the issues identified in section 3.4.1. 33

Annex: Report on the meeting of the experts on the 6th of December 2016

A.1. Background

This meeting was organized to support DG CONNECT Cybersecurity & Digital Privacy – Unit H1 on the definition of an European-wise security certification framework in various domains. The background of this meeting are the COMMISSION STAFF WORKING DOCUMENT Advancing the Internet of Things in Europe SWD(2016) 110/2 and the COMMISSION STAFF WORKING DOCUMENT Contractual Public Private Partnership on Cybersecurity & Accompanying Measures SWD (2016) 216 final, which recommended an improved level of security for IoT devices and applications (SWD(2016 110/2) and the definition of a framework for security certification and labelling in IoT.

In addition to the previous staff working documents, other organizations are also working on the definition of an European security certification framework for specific domains (e.g., IACS or IoT) or in general for cybersecurity products. For example, the European AIOTI (European Alliance of IoT Innovation) Working Group 4 has published a document on the security and privacy aspects of IoT[3] where it is advocated the need for a security certification framework at European level with the concept of IoT Trust label. In a similar way, The European IACS (Industrial Automation and Control Systems) has been working on a security certification framework for IACS products[4]. The European public private partnership on cybersecurity (cPPP) has also started to investigate a potential security certification framework[5].

We have also to consider that security certification is not a new concept. Actually, as described in previous sections of this report, security certification has a long history of more than 40 years. Then, it is not recommended to reinvent the wheel but rather to mitigate the risks and challenges still present in the most common security certification processes and standards (which has also been described in previous sections of this report).

Representatives of the ARMOUR project were also present at the meeting.

Within this context, an expert meeting was organized on the 6th of December 2016 to gather the feedback from security experts on the potential way forward for the definition of an European security certification framework. Experts and representatives from the organizations identified above were invited to the experts meeting to provide their views and the results of their work.

A.2. Participants

The list of experts invited to the meeting was following:

Name Surname	**Company**	**Representative of Organization/sector**
Eireann Leverett	IOActive	IoT
Jacques Olaf Kruse Brandao	NXP	cPPP, cybersecurity in general

[3] Report AIOTI Working Group 4 – Policy. http://www.aioti.org/wp-content/uploads/2016/10/AIOTIWG04Report2015.pdf

[4] European IACS Components, Cyber-Security Compliance and Certification Scheme https://erncip-project.jrc.ec.europa.eu/networks/tgs/european-iacs

[5] http://europa.eu/rapid/press-release_IP-16-2321_en.htm.

Arthur van der Wees	Arthur Legal	cPPP, cybersecurity in general
Dr Paul Theron	Thales	IACS
Mr Jean-Christophe Mathieu	Siemens	IACS
Philippe Cousin	Eglobalmark	IoT
Kai Rannenberg	Goethe Universitat	cPPP - IoT
Bruno Legeard	Université de Franche-Comté	IoT
Sergio Lomban	SGS	IoT,
Georg Stuetz	NXP	cPPP, cybersecurity in general

In addition, Gianmarco Baldini, Alessandro Lazari, Ignacio Sanchez from DG JRC, Domenico Ferrara from DG CNECT H1 and Aristotelis Tzafalias DG CNECT H1 were present at the meeting.

A.3. Agenda of the meeting

The agenda of the meeting was following:

Experts Meeting on security certification and labelling 6th of December 2016 Brussels avenue de beaulieu 25 - Conference Room 0/S 9		
09:00-09:30	**Welcome and Tour the table**	***European Commission, all*** ***Domenico Ferrara*** ***(DG CNECT)***
9:30 – 9:50	**Presentation by representative of ECSO**	***Sergio Lomban*** ***for ECSO***
9:50 – 10:10	**Presentation by AIOTI representative**	***Arthur van der Wees*** ***(Arthur Legal)*** ***for AIOTI***
10:10 – 10:30	**Presentation by Kai Rannenberg**	***Kai Rannenberg*** ***(Goethe University Frankfurt)***
10:30-11:00	**Presentation by IACS + Q&A**	***Paul Theron –***

		(Thales) and Alessandro Lazari (JRC E.2) IACS
11:00-11:20	**Coffee Break**	
11:20-11:40	**A way forward for security certification in Europe. Key elements and challenges**	***Gianmarco Baldini (JRC E.3) (presentation not given because of delay introduced by other presentations)***
11:40-12:00	**Model Based Testing**	***Philippe Cousin (Eglobalmark) Bruno Legeard (Université de Franche-Comté)***
12:00 – 13:00	**Discussion on how to address the key challenges for security certification in Europe Part 1**	***All***
13:00-14:00	**Lunch**	
14:00 – 15:00	**Discussion on how to address the key challenges for security certification in Europe Part 2**	***All***
15:00-15:30	**Summary of the results of the analysis and identification of the key actions**	***EC to coordinate, All to participate***

In the following section, are provided the presentations by each presenter and the related discussion:

A.4. Presentations and discussions

Sergio Lomban: The view from the European Cyber Security Organisation of cPPP

Sergio Lomban presented the view of Working Group 1 (Standardisation, Certification, Labelling, and Supply Chain Management) of ECSO. Mr Lomban explained that ECSO is now composed by many members (89 members) from different categories of stakeholders (government, manufacturers, service providers, certification bodies and so on).

The motivation for the work of WG1 were the following:

- Existing certification schemes can neither cope with the massive deployment and continuous maintenance of hyper-connected devices nor with the aggressive Time-To-Market situation.

- It is very important to continue with a strong focus on building upon existing unique European core expertise, such as the design, evaluation and certification of embedded devices.
- Until 2020 it is expected to have about 50 billions of IoT devices in the field. So-called physical attacks are becoming more and more relevant especially for devices which are physically accessible for an attacker. With the rise of IoT where cars communicate with each other or with critical infrastructures or where health applications are involved, such attacks will become even more dangerous as now human lives are at stake.

The objectives of WG1 are following:

- ECSO will develop a cyber security evaluation and certification framework for the benefit of the protection and security of the European citizen (made visible through a dedicated "label") and to increase the competitiveness of European industry.
- ECSO will include not only devices and products but also the ICT infrastructure, delivery of services and the continuous secure integration of devices and resulting products into larger systems.
- ECSO will draw special attention to the aspect of security & privacy by design including a minimal set of associated requirements to be covered throughout the entire ECO-system of cybersecurity.
- ECSO will take existing technology, company, process and people certification schemes into account including lessons learned regarding modern requirements (e.g. fast deployment and updates in the field, agile development, aggressive time-to-market, …).
- ECSO will ensure to have the appropriate level of flexibility of the certification framework allowing to customize certification towards the needs of different verticals (car, health, critical infra, home, …). This also allows to define appropriate mechanisms to protect the certification brand as well.
- ECSO aim to accomplish those tasks via a joint effort hand-in-hand with industrial, public sector, research and academic partners making sure to build upon Europe's unique security & privacy expertise.
- ECSO will leverage the capabilities and work with standardization, certification and normalization bodies while ensuring that the costs of evaluation, testing and certification and compliance does not significantly impact the cost negatively to the end customers.
- ECSO will provide a link to existing (e.g. NIS Directive, eIDAS Directive, GDPR regulations) and future regulations in the policy domain.

The roadmap of ECSO in 2017 will be:

- Evaluation of all existing testing/certification schemes across Europe and globally and to various properties such as product domain applicability, security assurance levels, type of vulnerability assessment, time to market, costs and agility.
- Benchmarking and identifying relevance of each existing scheme as per the requirements of both the public and private sectors.
- Mapping and developing opportunities for harmonization of existing schemes.

- Developing "best practices" solutions within the sub-areas, moving toward a "harmonized" approach to cyber security & privacy a consensus based environment.
- Working with public sector partners to address mutual recognition of "future" schemes.
- Accomplishing a "fast track" process to achieve actual standards.
- Implementing and piloting these testing and certification solutions to demonstrate effectiveness and cost efficiency as well as customer acceptance and trust.

After the presentation, it was discussed how ECSO can work together with the other groups (AIOTI, IACS and the European Commission) to create synergies and harmonize the different efforts.

Arthur van der Wees (Arthur Legal)

Dr Arthur van der Wees provided a multi-angle view about security and data protection in IoT . The presenter said that a multi-angle approach should be pursued because many different stakeholders may be involved. In addition, security experts should focus on the exposed devices: the ones with minor security capabilities or more exposed to external attacks. The rationale is that central infrastructures will be probably protected with physical security and powerful cryptographic solutions while IoT devices with limited power and storage capabilities will not have the same degree of protection. The presenter also linked security to safety in Cyberphysical systems (CPS) or IoT devices used in critical infrastructures. The presenter also supported a vision where security should be a solution rather than a problem also from a business/economic point of view. Better cybersecurity will enable new markets, promote innovation, and give consumers confidence to use new technologies that improve the quality of life. Poor security will likely cause the IoT market to eventually collapse on itself as consumers and other users begin to lose trust in technology from compilations of horror stories & market failure. The presenter also highlighted the need to address the patching process in security certification as software update will be quite common in IoT. He also stressed the value of monitoring of IoT devices after deployment.

Kai Rannenberg (Goethe University Frankfurt)

Prof Rannenberg focused on the complexity of the security certification process as shown in the figure below:

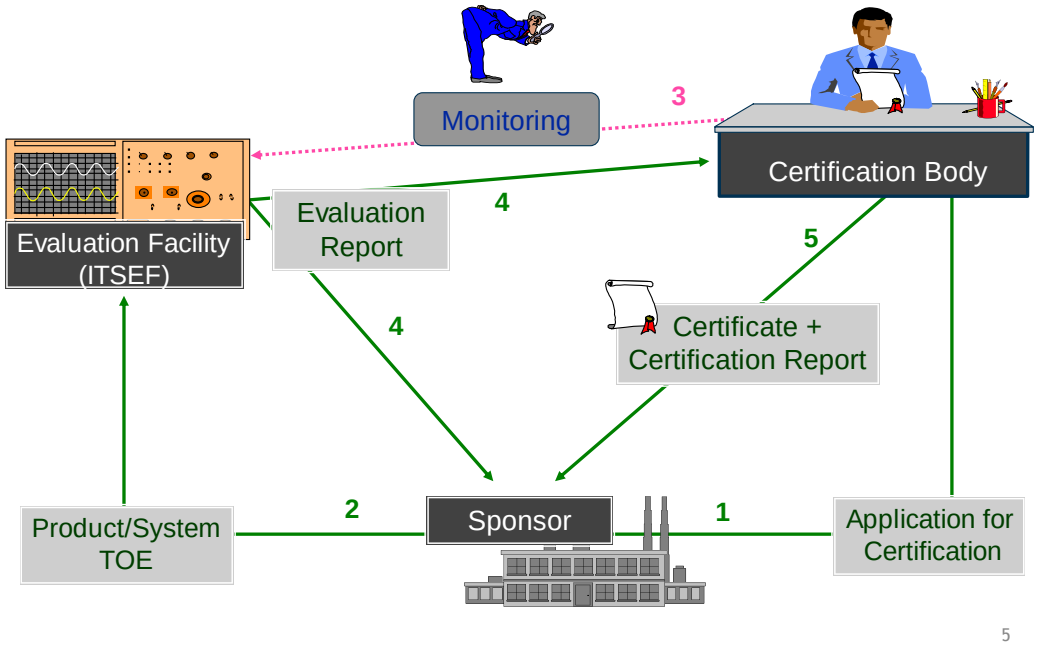

Figure 10 Security certification presented by Prof Rannenberg

Many different stakeholders are involved in the certification and evaluation process. The presenter also described the need for security certification: people use more and more complex technology to interact in the information society and the users need help or need to know what technology to trust:

- Does the offered system, product or service meet the requirements?
- Does it fulfil legal requirements?
- Is the given organization trustworthy?

Vendors‘ marketing information does not (always) help as it may be biased. Some kind of independent evaluation and certification is needed, which check products, systems, services or even organization and report on their security/privacy properties. A key issue is how to compare certification results.

From the user point of view, many existing ICT applications and products do not provide transparency on trust. The presenter cited a study from the Federal Ministry of Food, Agriculture and Consumer Protection that 37% of people who don’t use a smartphone, explain their refusal with a lack of trust in smartphone devices [6] and they do not have confidence that a smartphone application respects their privacy either. To this purpose the researcher team of the presenter conducted a study to monitor and analyse the behaviour application on a smartphone (project called Privacy4AppMarkets[7]). The application provides a privacy score on the users’ app-behaviour ratings. Regarding security certification and labelling, the presenter explained that certification and labelling based on meaningful evaluation is a useful investment but the questions are:

- Who pays and who sets priorities ?
- What to certify/label ?
- What is security in criteria ?
- Is privacy considered/included/covered ?

[6] BMELV 2012, Sicherheit und Datenschutz bei Smartphones, Hintergrundpapier zur Verbraucherumfrage vom Mai 2012. *Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz / Federal Ministry of Food, Agriculture and Consumer Protection (Germany).*

[7] Gökhan Bal, Kai Rannenberg, Jason Hong: Styx: Privacy risk communication for the Android smartphone platform based on apps' data-access behavior patterns; Pp. 187-202 in Computers and Security, Volume 53, September 2015, doi:10.1016/j.cose.2015.04.004.

From an economic point of view, the smaller the user (citizen/SME) is and:

- more is in need of help with the assessment of products
- more is in need of help with understandings certifications and the meaning of labels
- less budget (directly or indirectly) is seemingly available for certification

Then, the economics aspects are quite important.

Paul Theron (Thales)

Paul Theron from Thales provided a presentation on the activities of the IACS group, which has been going on for the last two years.

The starting points of the discussion are that:

- IACS & the IoT will be (are already) extremely pervasive & attractive to attackers
- The security of a system is far more complex than that of a component
- So many factors enter into account here (human, technical, physical, processes)
- This is why we have to start by building the foundations of cybersecurity. A SYSTEM will never be secure if its COMPONENTS are not.

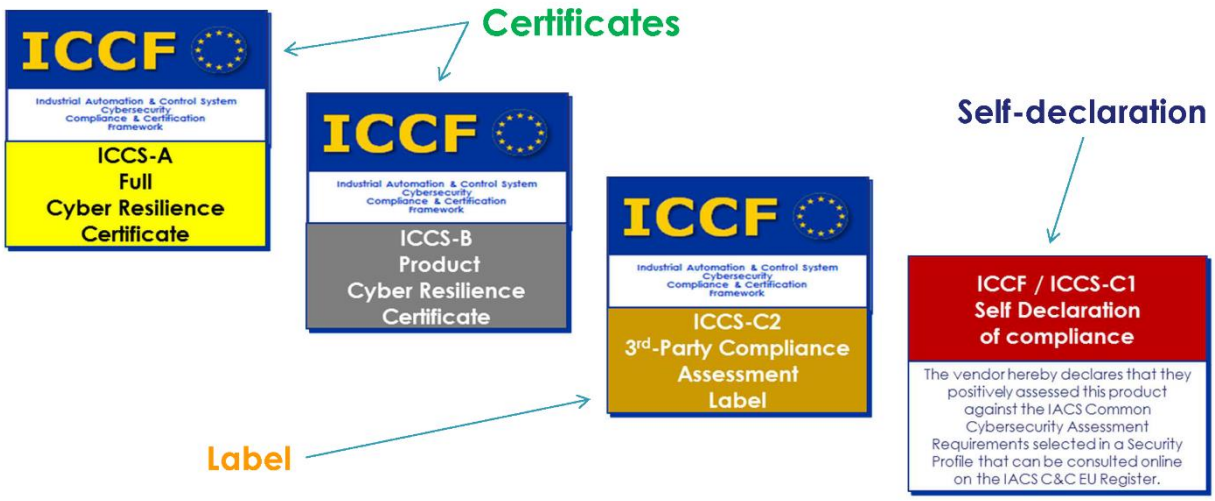

Figure 11 Four levels of certification in IACS

The four levels of certification defined in IACS are shown in Figure 11. The first two levels are the highest level of certification with intrusion testing or other high levels type of test (Cyber Resilience Testing). The last level is a self-declaration of compliance. The first two levels provides a certificate, the third a label and the fourth is a self declaration of compliance.

A technical report, which describes in detail the overall security certification process has already been published by the IACS group. The future steps in 2017 and 2018 are:

1. Global project management and stakeholder engagement;

2. Stakeholders recruitment and liaison (including national agencies, vendors, user industries, certifiers and labs);

3. A one day of ICCF training (for recruited pilot-participants, so as to introduce everyone to the ICCF mindset, concepts, upcoming challenges and vocabulary;

4. Focused pilot projects performed together with vendors, users, national cybersecurity agencies, (National) Labs and Accreditation & Certification bodies;

5. ICCS-A development process assessment;

6. ICCF governance body and processes;

7. Feedback and improvement of the ICCF

The conclusion of the presentation is that the security framework defined by IACS is already a mature process, which could be adopted in other contexts or domains.

Philippe Cousin (Eglobalmark), Bruno Legeard (Université de Franche-Comté): ARMOUR project for security certification in IoT and Model Based Testing

Philippe Cousing and Bruno Legeard provided a presentation on the Horizon 2020 ARMOUR project. The fundamental elements of ARMOUR are Model Based Testing (MBT) and TTCN-3. The first defines the model of the test bed configuration and devices to be tested, while the TTCN-3 test suite is used to implement the test execution.

The presenters believe that the ARMOUR approach could enhance the security certification process by addressing the following main issues, which are present in today certification processes:

1. How to make the testing part of the labelling and certification process cheaper ?
   - By building the process on reusable, configurable security test patterns and automated test generation.
   - By easing the work for certification bodies through a common model language, which can also be easy extended.
   - By directly correlating the certification scheme with the test patterns to be used.

2. How to ensure the quality and reproducibility of the assessment?
   - The security test patterns (models of MBT and test suites of TTCN-3) should be agreed by the certification authorities.
   - Test automation ensure the replicability of the test execution and test results.

3. How to deal with change?
   - Using the automated testing for continuous monitoring and testing at running stage to keep the certificate update. This means that the models could be used not only to support incremental testing but also to facilitate the monitoring of IoT devices after certification and deployment in the field.

Then, the presenters have shown an example of large scale testing, where these concepts have been applied:

TP ID	Security Test Patterns
TP_ID 6	Run unauthorized software
TP_ID 8	Resistance to eaves dropping and man in the middle
TP_ID 10	Resistance to Injection Attacks
TP_ID 11	Detection of flaws in authentication

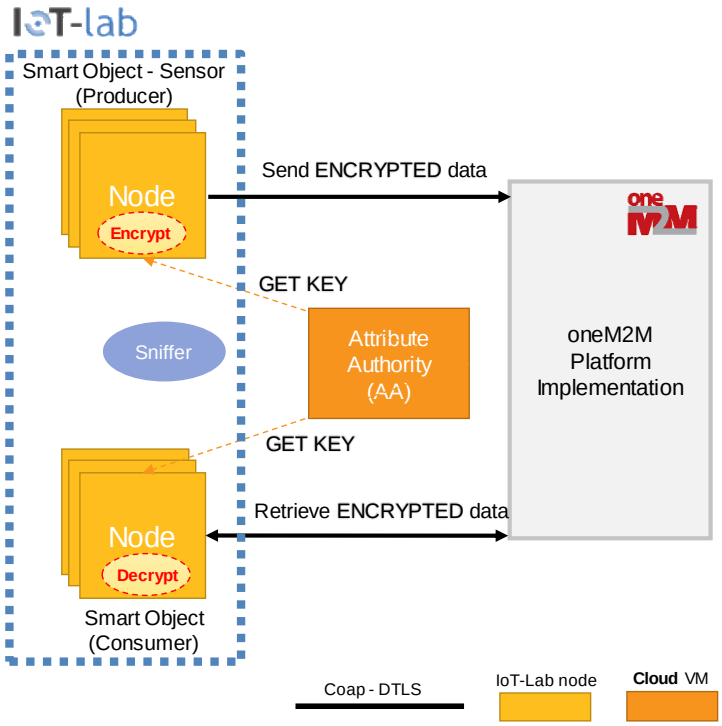

Figure 12 Examples of the application of the testing concepts of ARMOUR project.

In this example, test suites are executed against real IoT devices (based on oneM2M platform implementation) in an IoT test bed. The test bed has been previously modelled using MBT. This is to show that the concepts of ARMOUR are not abstract, but they are applied to real systems and devices.

Eireann Leverett of IOActive

Eireann Leverett of IOAactive provided a presentation on Standardisation and Certification of Safety, Security and Privacy in the 'Internet of Things.

The big challenges identified by the presenter were:

- Established non-IT industries usually have a static approach with pre-market testing to standards that change slowly if at all. The time constant is typically a decade
- Malicious adversaries who can scale bugs into attacks mean we need a dynamic approach with patching, as in IT. The time constant is typically a month

To address these challenges and the need to improve security of IoT products in domains where security threats become safety hazards (e.g., healthcare, road transportation, cyber-physical systems), the presenter provided a set of detailed recommendations:

- Update Product Liability Directive to cope with systems that involve multiple products and services.
- Require vendors to self-certify, for their CE mark, that products are secure by default. This self-certification can be updated if needed to an higher level of certification in a second phase.
- Update NIS Directive to report breaches and vulnerabilities to safety regulators and users.
- Move safety standards bodies towards assessing security and safety together.

- Safety regulators should require a secure development lifecycle with documented vulnerability management following ISO 29174 and ISO 30111 at a minimum
- There is the need move from certifying single products to support the assurance of whole systems including the lifecycle and patch cycle
- Create a European Security Engineering Agency to support policymakers and regulators.

A.5. Discussion

After the presentations, there was an extensive discussion on how to integrate the different approaches and how it should be the way forward. One of the objectives of the discussion was to identify the main work items and actions items to support DG CNECT in the definition of a roadmap for security certification in Europe.

The following items were identified, grouped by categories:

1. Starting point: Which framework to start from ?

It was agreed that the definition of the framework should be based on the following main requirements and features:

- Scalable and flexible framework to foster harmonization of evaluation at European level;
- Flexible choice of reference standards (e.g. sectorial, procurement driven) for security certification. This means that common criteria may be adopted for some domains but other security certification schemes like CSPN could be adopted in other domains.;
- The same framework model to be promoted all over EU;
- Application of concepts from ARMOUR like Model Based Testing and TTCN v3;
- Metrics of evaluation and security requirements are identified by the domain's stakeholder. In other words, the benchmarks are domain specific.
- Human factor has to be considered in the definition of the security profiles. In other words, the security profiles could be adapted to the context where the ICT product or device is used.
- Certification effort should be proportional to the objective (kind of use) of the product.

2. Economics of security. Who is going to pay for the security certification costs ?

This topic is focused on addressing the problem of economics of security where users do not purchase the most secure products because they are more expensive than others. In this topic, it was agreed to focus on the following work items:

- Case by case issue. Very dependent on the image factor of the manufacturer;
- Mass market Vs. specific client. Mass market may be based on different security certification levels (self-certification) than specific clients or domains (e.g., energy critical infrastructures).
- Investigate if a procurement-driven approach by government could support the bootstrap of the security certification framework.
- Disrupt the economic model of the attackers. Prioritize the security certification on the threats, which give economical gains to the attackers and mitigate these threats.

3. Prioritization of domains (there's no consensus and the question is unclear)

This topic was related to a discussion on the prioritization of the domains. In other words, the security certification framework should be applied to which domains in a first

phase. In addition, the security framework should be focused on products certification, applications or service certification ? The following items/considerations apply:

- Consumer protection Vs. Critical Infrastructures. The item is related to the choice of focusing in a first phase to consumer mass market products for consumer protection or on critical infrastructures.
- Avoidance of social dislocations is the key. The priority could be based on the social impact and disruption (e.g., weak categories of citizens, financial fraud).
- IPR. The priority could be based on the protection of Intellectual property rights.
- Highly sensitive data. The priority could be based on the protection of sensitive data.
- Safety related (e.g. transportation). The priority could be based on the mitigation of safety risks. This means that high priority domains could be transportation, energy or cyber-physical systems.
- Anybody too small to assess security by themselves. The priority could be on the support of small companies or users, who do not have the capabilities to protect themselves in an adequate way (e.g., SME).

4. Security and Privacy

The discussion was on the need to support security certification both for security and privacy requirements.

- It was agreed that we need to refer to the GDPR and investigate further how privacy requirements could be jointly implement with security requirements.

5. Certification based on the processes (e.g., development processes)

The discussion was on the possibility to include the development process (white box testing) as part of the certification but there was no agreement.

6. Governance

- Short, practical steps toward a European Governance should be investigated

7. Role of specific regulations in each domain? What about Radio Equipment Directive (RED) and other regulations/directives ?

- Landscaping the relevant certifications
- Avoid perverse incentives by understanding the regulatory environment before changes for security and privacy.

8. Dynamic changes of products (e.g. patches)

The discussion was focused on how to better support changes of the products like patching.

- Related to the lifetime support of the product
- Product to be recertified only when a substantial change is applied

- What is more valuable? Fast patching or keeping certification valid? Depending on type of products (domain specific).

9. Is a voluntary approach self-sustainable?

   - Encouraging stakeholder should lead to voluntary engagement of certification
   - Potential issue of international law and market related agreements (import/export)

10. Only security certification of products or also systems and services, which are intrinsically more complex? (There was no clear consensus)

    - Focus on certification of products as certifying system is too complex at the moment
    - Modular approach starting from products
    - Two phases approach? We could focus on security certification first and then certification of application and services.
    - We need a definition of products, services and applications to better clarify the categories.
    - Post market monitoring can be useful ? The idea is that security certification could be complemented by monitoring of certified products and systems in the field.
    - Not every combination of products is more complex than single products.

11. How to align ECSO, AIOTI, SOG-IS, IACS, FIRE

    - Action on EC to coordinate the collaboration among the different organizations.

A.6. Conclusions of the meeting

The meeting was successful as it provided a list of work items and issues for the future roadmap on security certification. Each expert provided his opinion on how to define an European security framework for certifications. The overall consensus is that we have to strengthen the security and privacy of connected devices in the future and security certification could be one of the tools. A key aspect is related to harmonization of the security certification processes at European level to support the European Single Market for cybersecurity related products. It was also highlighted the need for complementary tools like the monitoring of the security products after post market deployment. The experience of IACS (Industrial Automation and Control System) in security certification is quite valuable because they have already worked on this topic for years and their lesson learnt could be quite valuable for the definition of a security framework in other domains as well. Another aspect was the distinction between security certification of products and services. Security certification of services or applications can be significantly more complex than security certification of products. At the end of the meeting, a list of key elements to investigate for the future roadmap on security certification and labelling was defined. This is an important input to DG CNECT.

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*)**:**

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

More information on the European Union is available on the internet (http://europa.eu).

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
  via EU Bookshop (http://bookshop.europa.eu);
- more than one copy or posters/maps:
  from the European Union's representations (http://ec.europa.eu/represent_en.htm);
  from the delegations in non-EU countries (http://eeas.europa.eu/delegations/index_en.htm);
  by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm) or
  calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

  (*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (http://bookshop.europa.eu).

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

Annex 9:

Mapping of cybersecurity sectorial initiatives

at the EU and international level

Deliverable prepared by the European Commission and ENISA for the Cooperation Group under NIS Directive within the context of the task 'Discussions related to the security measures for operators of essential services'

Version 2.0, last updated July 2017

Contents

I. ABOUT THIS DOCUMENT 6
II. INTRODUCTION 7
A. NIS Directive in a nutshell 7
B. Key horizontal actors at the EU level 9
III. ..... SECTORS 10
A. ENERGY SECTOR 10
B. TRANSPORT SECTOR.....15
1. Air Transport.....15
2. Land Transport (Rail & Road transport) 20
3. Maritime Transport.....22
C. FINANCE AND BANKING SECTORS 24
D. HEALTH SECTOR 29
E. DRINKING WATER SECTOR 32

I. ABOUT THIS DOCUMENT

➢ Context

The Directive on Security of Network and Information Systems (NIS Directive)[8] is a major milestone towards building cybersecurity resilience at the European level as it lays out the first EU-wide rules on cybersecurity. Its objective is to achieve a high common level of security of network and information systems within the EU.

The Directive creates the '**Cooperation Group**' between Member States, in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them.

Given that the NIS Directive gives the Member States a certain degree of discretion related to Directive transposition, the Cooperation Group will have a very important role in ensuring that the Directive is transposed and implemented in a convergent manner across different sectors as well as cross borders, to ensure coherent approach across the Union.

During the second informal meeting of the Cooperation Group on 25 October 2016 an agreement was reached on the initial working plan for the first year of work of the Cooperation Group. Among others, the European Commission and the European Network and Information Security Agency (ENISA) were tasked with presenting a **mapping of relevant sectorial initiatives** at the EU and international level in the field of cybersecurity to ensure that both the members of the Cooperation Group and relevant actors at the Member State level involved in the transposition process have a clear overview of work that has already been conducted in the field. This should help coordinate different efforts, ensure coherence and avoid duplication.

➢ About this paper

This document, prepared by the European Commission and ENISA, maps ongoing initiatives in the field of cybersecurity across key sectors covered by Chapter III of the NIS Directive: energy, transport, banking and finance, health, drinking water.

Each section presents the most relevant actors in the field - the European Institutions (including relevant experts groups), key agencies (EU and whenever relevant international) involved in the area as well as stakeholder organisations.

Each section also presents a brief policy and regulatory context and enlists key initiatives in the field. Whenever possible, links to relevant documents and information sources are provided to facilitate more detailed information search.

This document is conceived as "**a living document"** and will be regularly updated by the Commission services and ENISA to inform the Cooperation Group about any developments that might be relevant for the transposition process.

Please note that this document focuses on cybersecurity work and initiatives that might be directly related to the transposition of the NIS Directive as this is the main focus of the Cooperation Group work for the next months.

Moving forward and in case the Cooperation Members find it useful, this document could be also extended to take stock of other cybersecurity policy initiatives, which might have an indirect link to the implementation of the NIS Directive (cybercrime and cyber defence activities, cybersecurity market measures, training and education, etc.).

[8] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

II. INTRODUCTION

A. NIS Directive in a nutshell

The Directive on Security of Network and Information Systems (NIS Directive)[9] was formally adopted on 6 July 2016 and entered into force on 8 August 2016. Member States will have **21 months** to implement the directive into their national laws and **6 months** more to identify operators of essential services.

- **Cornerstones of the NIS Directive**

1) Improving National Cyber Security Capabilities

Member States are required to adopt a national NIS strategy defining the strategic objectives and appropriate policy and regulatory measures in relation to cyber security. Member States are also required to designate a national competent authority for the implementation and enforcement of the Directive, as well as **Computer Security Incident Response Teams** (CSIRTs) responsible for handling incidents and risks.

2) Improving Cooperation

The Directive creates '**Cooperation Group**' between Member States, in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them. The Commission provides the secretariat for the Cooperation Group.

The Directive also creates the **CSIRTs Network**, in order to promote swift and effective operational cooperation on specific cyber security incidents and sharing information about risks. **The EU Agency for Network and Information Security** (ENISA) provides the secretariat for the CSIRTs Network.

3) Security and Notification Requirements for Operators of Essential Services

Businesses with an important role for society and economy, referred in the Directive as "Operators of Essential Services", will have to take appropriate security measures and to notify serious incidents to the relevant national authority.

The Directive covers such operators in the following sectors (ANNEX II of the Directive):

- Energy: electricity, oil and gas
- Transport: air, rail, water and road
- Banking: credit institutions
- Financial Market Infrastructures: trading venues, central counterparties
- Health: healthcare providers
- Water: drinking water supply and distribution
- Digital Infrastructure: internet exchange points (which enable interconnection between the internet's individual networks), domain name system service providers, top level domain name registries

Member States will need to carry out a so-called **identification process** in which they have to define which entities mentioned in Annex II will fall under the scope of the NIS Directive. This identification process will be based on criteria laid down in the directive, such as whether the service provided by the entity is essential for the maintenance of critical societal or economic activities.

[9] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

4) Security and notification requirements for digital service providers

Important digital businesses, referred to in the Directive as "digital service providers" (DSPs), will also be required to take appropriate security measures and to notify incidents to the competent authority. The Directive will cover the following providers:

- Online marketplaces;
- Cloud computing services;
- Search engines

Table 1: NIS Directive Transposition & Implementation Timeline

Date	Entry Into Force +	Milestone
Dec. 2016	4 months	Submission of the draft of the first implementing act laying down the procedural arrangements necessary for the functioning of the Cooperation Group to the Network and Information Systems Security Committee[10]
Feb. 2017	6 months	Cooperation Group and CSIRT network begin to perform their tasks
Aug. 2017	12 months	Adoption of implementing acts related to the security and notification requirements for DSPs[11]
Feb. 2018	18 months	Cooperation Group establishes work programme
May 2018	21 months	Transposition into national law
Nov. 2018	27 months	Member States to identify operators of essential services
Nov. 2018	27 months	Member States to submit information to Commission necessary to enable the Commission to assess the implementation of the Directive, in particular the consistency of Member States' approaches to the identification of operators of essential services.
May 2019	33 months (i.e. 1 year after transposition)	Commission report assessing the consistency of Member States' identification of operators of essential services
May 2020	45 months	Member States to review and, where appropriate, update the list of identified operators of essential services
May 2021	57 months (i.e. 3 years after transposition)	Commission review of the functioning of the Directive, with a particular focus on strategic and operational cooperation, as well as the scope in relation to operators of essential services and digital service providers

[10] Pursuant to Article 11 (5) of the NIS Directive, the formal deadline for the submission of the first draft is 9 February 2017. The Commission's intention with this early submission is to have the procedural arrangements adopted before the formal launch of the Cooperation Group so that a swift functioning of the Group is ensured from the very beginning.

[11] A first rough draft of the implementing act is planned to be presented to the members of the NIS expert group (which includes representatives of Member States advising the Commission) by end of December 2016 / January 2017.

B. Key horizontal actors at the EU level

In order to avoid repetition, the roles of horizontal actors in the EU-level cybersecurity landscape are described below. Their work applies to all sectors presented in the rest of this document.

The Directorate General for Communications Networks, Content and Technology, or **DG Connect** is the Directorate-General of the European Commission responsible for managing policy, regulation and research in the area of information and communication technology. DG Connect and, particularly, its Cybersecurity and Digital Privacy Unit (Unit H.1), is the entity responsible for the support to the transposition and implementation of the NIS Directive and provides Secretariat for the Cooperation Group.

This Unit is also responsible for the contractual Public Private Partnership on cybersecurity, which was signed in July 2016 with the cybersecurity industry represented by the European Cybersecurity Organisation. One of the working groups under the partnership will focus on sectorial dimension of cybersecurity.

ENISA is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA's relevant work across different sectors is mentioned in relevant sections of this document.

The NIS Directive envisages an important supporting role for the Agency for the transposition and implementation of the NIS Directive. In particular, ENISA provides the secretariat to the CSIRTs network, the cornerstone of operational cooperation, and it is also called to assist the Cooperation Group, dealing with strategic cooperation, in the execution of its tasks.

III. SECTORS

A. ENERGY SECTOR

The energy infrastructure is inarguably one of the most complex and most critical infrastructures of a modern society and serves as the backbone for its economic activities and for its security. Given that the energy sector delivers crucial inputs to other sectors, there are important implications also for other parts of the economy.

One of the particularities of the traditional energy sector are its operational technologies, which are historically composed of control systems specifically tailored to operate the physical networks. However, through the increasing shift towards renewable energies and decentralised production, the energy sector of today is undergoing a very rapid change in terms of infrastructure and market.

Digital technologies play an increasingly important role in the energy sector. An ever smarter energy system can perform power generation, transmission, network management and marketing related tasks with much better precision and faster response times than human- dependent systems, thereby saving energy, prioritizing usage, and setting policies for quick response to outages.

But the new efficiency in supply services comes at a price: increased exposure to cyber-attacks and a higher risk for personal data. In a truly cross-sectorial manner, these threats apply to all - generation, transmission and distribution technologies, and to energy market services.

Therefore, ensuring resilience of the EU energy supply system against cyber-threats is becoming increasingly important as wide-spread use of IT and data traffic becomes the foundation for the functioning of infrastructures underlying the energy system.

- **Relevant European Commission DGs**

- The **Directorate-General for Energy** (**DG ENER**)[12] focuses on developing and implementing policies aiming to deliver a secure, sustainable, and competitive energy for Europe. In particular:

1.

  - The **Smart Grids Task Force** was set up by DG ENER in 2009 to advise on policy and regulatory issues related to smart grid deployment and development. It consists of five Expert Groups which focus on specific areas. Expert Group 2 aims to mitigate the risks to personal data and security of smart metering systems. This Working Group, under the supervision of DG ENER and DG Joint Research Centre (JRC), has delivered in October 2016 a report on the Identification and Selection of Best Available Techniques[13] that addresses risks related to privacy and security.
    As a direct action of the Commission Communication "Clean Energy for All Europeans" (COM/2016/0860 final), the European Commission set up a stakeholder working group under the Smart Grids Task Force in spring 2017 to prepare the ground for a network code on energy-specific cyber security until end of 2018.

  - From December 2015 to February 2017, the Energy Expert Cyber Security Platform (EECSP)-Expert Group analysed the energy specific needs in terms of cyber security. This group, set up by DG ENER in cooperation with other Commission services, identified the challenges and the specific needs of the

[12] https://ec.europa.eu/energy
[13] https://ec.europa.eu/energy/sites/ener/files/documents/bat_wp2_techniques_mapping_and_clustering.pdf

energy sector not currently covered under EU legislation. The final report – aiming to advice DG ENER – was published February 2017 at the Commission Website[14].

2.
   - In spring 2017, DG ENER launched a study on the evaluation of risks of cyber incidents and on costs of preventing cyber incidents in the energy sector. The subject matter of the study is to provide a risk assessment of cyber threats in the energy sector as well as an analysis of existing or planned measures to mitigate these risks and their implementation and operational costs. It is planned to finalise and publish the study in the second half of 2018.

- **DG Joint Research Centre (JRC)** supports EU policies providing independent evidences and advices throughout the whole policy cycle. DG JRC's activities also cover the energy and cyber-security sectors.

  DG-JRC conducts experimental and research activities in the cyber-security and data protection of the Energy Sector. This includes cyber-security research on smart-metering systems, energy Generation, transmission and distribution infrastructures, the interactions between the grid and smart-home devices, as well as the analysis of the cybersecurity maturity of new energy architecture paradigms (renewable energy micro-grids, distributed ledgers based approaches etc). To conduct its on-field research activities JRC take advantage of some dedicated laboratories and platforms:

  - The Energy Distributed Ledger platform
  - The Cyber-Security Open Space Laboratory
  - The Energy Smart-Grid interoperability laboratory
  - The Experimental Platform for ICT Contingencies (EPIC)

3.

Moreover, JRC run also the **Thematic Network on Critical Energy Infrastructure Protection (TNCEIP)[15]** - an initiative of DG ENER, run by DG JRC - made up of European owners and operators of energy infrastructure in the electricity, the gas and the oil sectors. It allows energy sector operators to exchange information on threat assessment, risk management and cyber security.

➢ **Relevant EU Agencies**

EU policy activities in the **energy sector** are undertaken by the Commission in cooperation with EU Agencies.

ENISA supports the EU's initiatives in the field of cybersecurity through awareness raising activities and technical reports. In the energy field, ENISA has, for example, published a report on Smart Grid Security Certification in Europe[16].

ENISA has published several reports regarding Smart Grids[17], including:

- Smart Grid Security Certification in Europe
- Smart Grid Security: Recommendations for Europe and Member States
- Appropriate security measures for smart grids
- Communication network interdependencies in smart grids

[14] https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf
[15] https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure

17 https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids

ENISA has also published several reports related to ICS/SCADA[18], including energy aspects:

- A study on Communication Network Interdependencies in ICS/SCADA[19]
- Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors
- Certification of Cyber Security skills of ICS/SCADA professionals
- Good Practices for an EU ICS Testing Coordination Capability
- Window of exposure… a real problem for SCADA systems?
- Can we learn from SCADA security incidents?

Finally, in 2016 ENISA conducted a preparatory study regarding the identification criteria of Operators of Essential Services (OES). ENISA's on-going work for 2017 in the Energy Sector envisages the following reports (to be published in 2017)

- Security measures for OES
- Incident reporting requirements for OES
- Methodology for the identification criteria of OES

The European **Agency for the Cooperation of Energy Regulators** (ACER) aims to complement and coordinate the work of national energy regulators at EU level. Among others, ACER supports the implementation of cybersecurity regulation at national level. It also advices the European Commission on the development of network codes for gas[20].

➢ **Key external European organisations/stakeholder fora in the Energy sector**

- **Council of European Energy Regulators** (CEER)[21]: is a non-profit association which represents the interests of the energy national regulators in the EU. CEER has a dedicated Work Stream on cybersecurity through which national regulators aim to promote exchange of best practices in this area.

- **European Safeguards Research and Development Association** (ESARDA)[22]: is an association of European organisations in the area of safeguards which provides a forum for the exchange of information between nuclear facility operators, safeguards authorities and research bodies. The Commission is fostering regional and international cooperation on cybersecurity in the framework of ESARDA.
- **European Network of Transmission System Operators for Electricity** (ENTSO-E)[23]- **European Network of Transmission System Operators for Gas** (ENTSO-G)[24] represent the interests of transmission system operators for electricity and gas. Both organisations have an interest in cybersecurity, among others. For example:

    - ENTSO-G advises the European Commission on the development of network codes for gas[25].

    - ENTSO-E covers cybersecurity in one of its major projects such as Emergency and Restoration[26] and Regional Security Coordinators[27]. In addition, members of ENTSO-E undertake regular training sessions on how to respond quickly to

18 https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada
19 https://www.enisa.europa.eu/publications/ics-scada-dependencies
20 https://ec.europa.eu/energy/en/topics/markets-and-consumers/wholesale-market/gas-network-codes
21 http://www.ceer.eu/portal/page/portal/EER_HOME
22 https://esarda.jrc.ec.europa.eu/
23 https://www.entsoe.eu/Pages/default.aspx
24 http://www.entsog.eu/
25 https://ec.europa.eu/energy/en/topics/markets-and-consumers/wholesale-market/gas-network-codes
26 https://www.entsoe.eu/major-projects/network-code-development/emergency-and-restoration/Pages/default.aspx
27 https://www.entsoe.eu/major-projects/RSC/Pages/default.aspx

any potential attacks and how to protect critical infrastructures[28] .

- **European Associations for Distribution System Operators:** there are four European associations representing electricity distribution system operators, (CEDEC[29], EDSO[30], EURELECTRIC[31] and GEODE[32]). Relevant activities in the field of cybersecurity include:
    - Partnerships with relevant stakeholders. For example, in 2016 EDSO and the European Network for Cyber Security (ENCS) signed a Memorandum of Understanding on knowledge exchange for security regulations, effective cyber security practices and standardisation for energy distribution companies[33].
    - Publication of reports such as Smart grid cybersecurity[34].
    - Organisation of events such as Cybersecurity in Electricity Distribution Grids[35].

4.

- **Incident and Threat Information Sharing EU Centre** (ITIS-EUC)**[36]**: it collects analyses and disseminates information on incidents and vulnerabilities in the energy sector, with the aim to improve the situational awareness of Critical Energy Infrastructures (CEIP). ITIS-EUC relies on a web application through which members (European Agencies and Institutions, TSOs, DSOs, utilities from the gas, electricity and oil sector, etc.) share relevant information.

- **European Energy – Information Sharing Analysis Center[37]** (EE-ISAC): the EE-ISAC was created as result of the DENSEK project[38] (Distributed Energy Security Knowledge) launched by DG Home of the European Commission in 2015. The EE-ISAC provides a platform for members to share information on cyber security and cyber resilience in the energy sector. Members include European utilities, service providers, academia as well as governmental and non-profit organizations

5.

➢ **<u>Key Agencies and Organisations at international level</u>**

- **The International Energy Agency** (IEA) is an intergovernmental organisation established in the framework of the OECD**.** It comprises of 29 member countries. Relevant activities in the field of cybersecurity include:
    - Roadmap for the development of smart grids, which also cover cybersecurity aspects[39]
    - Participation in the G7 Workshop on Cyber Security in the Energy Sector[40]

[28]https://www.encs.eu/2016/12/01/entso-e-participants-trained-to-better-defend-the-critical-infrastructure-from-cyber-attacks/
[29] http://cedec.com/
[30] http://www.edsoforsmartgrids.eu/
[31] http://www.eurelectric.org/
[32] http://www.geode-eu.org/
[33] http://www.energycentral.com/c/iu/edso-encs-join-forces-cybersecurity-standardization-europe
[34] http://www.eurelectric.org/media/304600/smart_grid_cyber_security_report-2016-030-0652-01-e.pdf
[35] http://www.eurelectric.org/events/2015/cybersecurity-in-electricity-distribution-grids/
[36]https://ec.europa.eu/jrc/en/scientific-tool/incident-and-threat-information-sharing-eu-centre-energy-sector-itis-euc
[37] http://www.ee-isac.eu/
[38] http://www.densek.eu/
[39] https://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf

The **International Atomic Energy Agency** (IAEA)[41] works to promote the safe, secure and peaceful use of nuclear technologies. Though established independently of the United Nations, the IAEA reports to both the UN General Assembly and Security Council. It has set up a **Computer Security Programme** aiming to provide its Member States with expertise and guidance at all stages of the development of an information and computer security programme. As part of this programme, the Agency conducts advisory missions and trains inspectors[42].

- **EU Policy & Regulatory environment**

The Energy and Climate for 2030[43] and the Energy Security Strategy[44] are the main EU policy and regulatory framework in this area and cover the internal and external dimension of energy policy. As regards the internal energy market, the creation of Energy Union is a priority of the Junker's Commission. Launched in February 2015, it covers various five dimensions: energy security, solidarity and trust; a fully integrated European energy market; energy efficiency contributing to moderation of demand; decarbonising the economy; and research, innovation and competitiveness. The aim of the Energy Union is to lead to a sustainable, low carbon and environmentally friendly economy, putting Europe at the forefront of renewable energy production and the fight against global warming. In light of the increasing digitalisation of the energy sector, the Commission intends to develop the Energy Union in synergy with the creation of the Digital Single Market agenda. This includes taking measures to ensure privacy protection and cyber-security.

The recent (2016) Directive on Security of Network and Information Systems (NIS Directive) put specific obligations on providers of essential services including the energy sector (electricity, oil, gas). The EECSP-Expert Group (12/2015-02/2017) was set up to advice the Commission and to reinforce the implementation of the NIS Directive at energy sector level. The group identified the challenges and the specific needs of the energy sector that are not currently covered under EU legislation and proposed the way forward to secure energy systems that provide essential services to European society.[45]

At the same time, cybersecurity has also started to be mainstreamed in energy-specific policy and regulatory initiatives. In 2016, the European Commission presented a package of measures to keep the European Union competitive as the clean energy transition is changing global energy markets. This "Clean Energy for all Europeans" package of 30 November 2016 acknowledges the importance of cyber security for the energy sector, and the need to duly assess cyber-risks and their possible impact on the security of supply. The "Clean Energy for all Europeans" proposals will also require the adoption of measures to prevent and mitigate the risks identified as well as further technical rules for electricity (i.e. a Network Code) on cyber-security to be adopted in the future. The revised security of gas supply regulation also acknowledges the importance of cyber security in gas.

---

[40] https://www.iea.org/media/topics/engagementworldwide/g7/IEAPresentationonCybersecurityatG7.pdf
[41] https://www.iaea.org/
[42] https://www.iaea.org/topics/computer-and-information-security
[43] http://ec.europa.eu/clima/policies/strategies/2030_en
[44] https://ec.europa.eu/energy/en/topics/energy-strategy/2030-energy-strategy
[45] Final report: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

B. TRANSPORT SECTOR

The present section focuses on cybersecurity in the three subsectors of the transport sector, namely air transport, maritime transport and land transport (rail and road transport).

- **Key highlights for transport sector**

Transport is one of the sectors especially vulnerable to cyber-attacks, in particular through the increasing use of electronic data communication. Digitalisation is expected to become a major enabler of the much needed transformation of today's transport system. The digitalisation in the transport sector is a critical feature in the effort to improve the efficiency and connectivity of transport, and ranges from the design of specific complex IT architectures to the use of off-the-shelf IT products. Transport moves people and goods, therefore and contrary to other sectors that may be also prone to cyber-attacks any failure might have serious consequences including massive loss of lives.

1. Air Transport

There is a general consensus among the aviation community that the air transport system needs to be protected against cyber-incidents, and there is a need to provide a holistic response at EU level, which is based on existing policies (such as the EU Cybersecurity Strategy, NIS Directive, EASA Basic Regulation, SES, AVSEC rules) and will be done in close coordination with other parties (Member States, ICAO, ECAC, and like-minded countries).

- **Relevant EU Institutions and other actors**

The **European Commission**[46] works together with Member States and stakeholders in addressing vast array of transport policies. Cyber security and cyber resilience in different modes of transport is an emerging issue.

The Commission's Aviation Strategy for Europe[47] highlighted the increasing vulnerability of the aviation system to cybersecurity or cyber safety risks and the need for the Commission and the **European Aviation Safety Agency** (EASA, see below) to address cyber risks for the aviation system. It also insisted on the need for EASA to cooperate with other competent bodies to this effect and proposed to clarify and strengthen EASA's role in the area of cybersecurity under the New Aviation Safety Regulation.

There are a number of regulatory committees and advisory groups the Commission is closely cooperating with, where resilience and cyber security issues are addressed. For aviation these are:

- **Regulatory Committee for Civil Aviation Security** (AVSEC)[48] is addressing the evolving threat to civil aviation. Appropriate authorities (e.g. Civil Aviation authorities, Ministry of transport, etc.) of each Member State are represented including observers from EEA states and ECAC[49].

[46] The department in charge within the European Commission is the 's Directorate-General for Mobility and Transport (DG MOVE), cf. http://ec.europa.eu/transport/index_en.htm
[47] COM (2015) 598 final
[48] created by Article 19 of Regulation (EC) No. 300/2008
[49] European Civil Aviation Conference

- **Stakeholders Advisory Group on Aviation Security** (SAGAS)[50], is a formally constituted consultation body that meets approximately 4 times a year, shadowing meetings of AVSEC. It consists of European representative organisations engaged in or directly affected by aviation security including Member States. SAGAS members are very active in the field of cyber security and a re-occurring point on cyber in aviation is regularly on its agenda.

6.

➢ **Relevant Agencies, Key external EU actors and International Organisations**

EU policy activities in **air transport** are undertaken by the Commission also in close cooperation with other bodies such as:

- **European Aviation Safety Agency** (EASA)[51] is an agency of the European Union (EU) with regulatory and executive tasks in the field of civilian aviation safety.

The vulnerability of the aviation system will significantly increase with the implementation of new technologies, with the use of commercial off the shell software, e-enabled technologies and increasingly interconnected transport and air traffic management systems. Against this background, EASA, in close cooperation with the Commission, developed a roadmap on cyber security[52] in aviation that follows the Commission priorities outlined in the 2015 Digital Single Market Strategy[53] and in the 2013 EU Cybersecurity Strategy.

As a first concrete measure EASA launched a screening of the current rules and practices in aviation and carried out a preliminary impact assessment of underlying rules related to modern aircraft design structures as regards their vulnerability to cyber-attacks.

Furthermore, EASA intends to set up the so-called European Centre for Cyber Security in Aviation (ECCSA) which will build on cooperation with all actors involved from both public and private sector: Member States, airlines, manufactures of aircraft, avionics and ground systems, airports, ANSPs. A link with ENISA[54], with law enforcement authorities (E3C[55])and intelligence (INTCEN) is also envisaged.

A Memorandum of Understanding with EU-CERT[56] that has been signed constitutes the 'engine' of ECCSA, i.e. it will provide secured IT infrastructure, but also cybersecurity tools and management services. This shall allow ECCSA to offer specific services to its constituents such as an assessment of cyber incidents and assistance for coordinating the response.

The Roadmap for cooperation between EASA and Eurocontrol also contains a detailed description of the activities led by both organisations in the field of cybersecurity.

---

[50] created by Article 17 of Regulation (EC) No. 300/2008

[51] https://www.easa.europa.eu/

[52] The Roadmap outlines the main areas for action. Two key elements of the programme can be highlighted: (i) creation of the European Center for Cybersecurity in Aviation (ECCSA): This new sectorial structure is intended primarily to serve as a cyber-threat and incident information management platform. Beyond its primary role it is also intended to take proactive, preventive action such as awareness raising or detection. It is foreseen that Members of ECCSA act as key cybersecurity experts in different aviation industry domains, including manufacturers, operators and ANSP; (ii) Rulemaking activities: the proposal for a new Aviation Safety Regulation (foreseen as a successor to current Regulation (EC) No 216/2008) suggests to strengthen the role of EASA. A revision of the relevant implementing regulations covering all domains of the aviation sector (design, manufacturing, maintenance, operation, ATM, airports, licensing) has been launched by EASA and is expected to result in amendments, by the Commission, of existing rules by 2018.

[53] COM(2015) 195 final

[54] European Network and Information Security Agency

[55] Europol's cybersecurity branch

[56] Computer Emergency Response Team for the EU institutions, bodies and agencies

In parallel, the Commission proposes in the amended Aviation Safety Regulation[57] to clarify the role and mandate of EASA related to cyber security and to outline essential cyber security requirements.

- **Single European Sky Air Traffic Management Research** (SESAR)[58]

The SESAR Joint Undertaking (SJU) study on a cybersecurity strategy in aviation[59] concluded on a number of recommendations which need to be followed in the development and deployment of the future Air traffic management system. Currently, SJU is preparing internal standards to ensure that the risks related to cybersecurity are appropriately addressed in all projects. Cybersecurity is now an integral part of the new EU ATM Master Plan[60] and of the SESAR 2020 Work programme. In addition, the SESAR Deployment Manager addresses cybersecurity in SESAR implementation activities following the Deployment Programme specific requirements.

In this light, modernisation of the EU ATM infrastructure will mean that cyber security is taken into account in the design, right from low maturity levels to the actual deployment of the technology.

- **European Civil Aviation conference** (ECAC)[61]

ECAC Cyber study group produced a working paper including the new ECAC Document 30 Recommendations on cyber security and guidance material on security response measures to cyber risks, utilising Member State and industry input. The work of the study group is the result of a joint collaboration between various national bodies and authorities, associations, agencies and experts in the field of ATM and safety.

- **International Civil Aviation Organisation** (ICAO)[62]

The 39th ICAO Assembly held in autumn 2016 adopted Cybersecurity Resolution A39-19, based on a joint EU-US submission[63]. It insisted mainly on the need for a holistic approach on cybersecurity involving all domains and for sharing information/best practices at ICAO level. The paper received unanimous support while it recognised that a consistent and coherent strategy for managing cyber threats and risks still needs to be developed. Furthermore, ICAO organised a Cyber security summit in April 2017[64].

The European Commission works with like-minded countries on a meaningful follow up to the ICAO's Cybersecurity Resolution A39-19 and the recent summit. Clearly, there is the need for a consistent and coherent global strategy.

- **EUROCONTROL**

Eurocontrol[65] is a European intergovernmental organisation. Its aim is to run safe, efficient and environmentally-friendly air traffic operations throughout Europe and to build a Single European Sky that will deliver the air traffic management (ATM) and improve the system's performance in the medium- and long-term.

---

[57] Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC, OJ L 79, 19.3.2008, p. 1–49

[58] http://www.sesar.eu/

[59] http://www.sesarju.eu/newsroom/all-news/study-details-rd-roadmap-atm-cyber-security

[60] Air Traffic Management

[61] https://www.ecac-ceac.org/ comprising of 44 European states, DG MOVE is an observer in the study group

[62] International Civil Aviation Organisation, a specialised UN Agency www.icao.int

[63] http://www.icao.int/Meetings/a39/Documents/WP/wp_493_en.pdf

[64] The ICAO Cybersecurity summit and exhibition, a joint safety and security event with the theme "Making sense of cyber" took place on 4-6 April 2017 in Dubai, UAE.

[65] https://www.eurocontrol.int/

When talking about the role of EUROCONTROL in cyber security, there are different aspects to consider. From the Network Manager perspective, EUROCONTROL has a resilience, monitoring and response role. EUROCONTROL is also responsible for crisis response activities. In this regard, through its European Aviation Crisis Coordination Cell, it ensures a proper coordination and response to crisis, including those deriving from cyber-incidents, impacting the EU aviation network.

In terms of non-operational tasks, EUROCONTROL is engaged in raising awareness around cyber-security related issues and supporting Member States in the oversight of ATM security. In addition, EUROCONTROL's training centre in Luxembourg[66] allows for the organisation of ATM security training activities.

Cybersecurity is part of the NEASCOG[67] work programme, which is aimed at developing a cyber-defence policy and recommending the cyber security base line for ATM. But it is also a part of the Education, Awareness and Training plan, which includes 'Promoting awareness through workshops and seminars on topics of interest.

In the context of the Centralised Services (CS)[68] currently under development, the CS 6-7 includes the deployment of a European ATM CERT (Computer Emergency Response Team) and a SOC (Security Operations Centre). The ATM CERT main functions are to collect, generate and distribute ATM relevant cyber intelligence and coordinate pan-European ATM response to ATM relevant cyber-security events/incidents. It will work in coordination with EASA ECCSA.

- **<u>EU/International regulatory and policy environment</u>**

- **ICAO Chicago Convention, Annex 17**[69]

7.

- **ECAC Doc 30, guidance material**

8.

- **Regulation (EC) No 300/2008** of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002[70]

9.

- **Commission Regulation (EU) No 18/2010**[71] regards Common specifications for the national quality control programme in the field of civil aviation security

10.

- **Commission Regulation (EU) No 72/2010**[72] regards the Minimum Standards on Aviation Security

11.

- **Commission Implementing Regulation (EU) No 2015/1998**[73] which sets out the detailed measures for the implementation of the common basic standards for safeguarding civil aviation against acts of unlawful interference that jeopardise the security of civil aviation

12.

[66] Accredited as Regional Training Centre of Excellence by ICAO

[67]The NEASCOG was jointly created by Eurocontrol and NATO in the aftermath of 9/11 as the European forum for ATM security in response to new and evolving threats to ATM. It is a civil/military forum bringing together ATM regulators, security authorities and Military from Member States, including NATO Partners (e.g. Mediterranean Dialogue, Ukraine, Russia, etc.);ICAO, ECAC, EC, IATA, IFALPA, IFATCA, CANSO, ANSP, Industry, FAA, and NATO and EUROCONTROL Agencies and Units.

[68] https://www.eurocontrol.int/centralised-services

[69] http://www.icao.int/Security/SFP/Pages/Annex17.aspx

[70] OJ L 97/72, 9.4.2008

[71] OJ L 7, 12.1.2010, p. 3–14

[72] OJ L 23, 27.1.2010, p. 1–5

[73] OJ L 299, 14.11.2015, p. 1–142

- **Regulation (EC) No 1592/2002**[74] **which proposes to establish a uniformly high level** of civil aviation safety in Europe as part of creating the single European sky

13.

- **Regulation (EC) No 1108/2009**[75] which extends EASA's activities towards a "total system approach"

14.

- **Commission Implementing Regulation (EC) No 1035/2011**[76] regards common requirements for the provision of air navigation services. It is being revised in order to incorporate last ICAO recommendations for ATM operator's management system. It includes provisions on security management systems

15.

- **Commission Implementing Regulation (EC) No 923/2012**[77] regards common rules on air traffic flow management (ATFM)

16.

- **Commission Regulation (EU) No 677/2011**[78] regards detailed rules for the implementation of air traffic management (ATM) network functions

17.

- **Commission Regulation (EU) No 551/2004**[79] regards the organisation and use of the airspace in the single European sky

18.

- **Commission Regulation (EU) No 376/2014**[80] regards the reporting, analysis and follow-up of occurrences in civil aviation

19.

- **Commission Regulation (EU) No 73/2010**[81] regards requirements on the quality of aeronautical data and aeronautical information for the Single European Sky

Additional sources:

ENISA's report on the cybersecurity aspects for Smart Airports[82]

[74] OJ L 240, 7.9.2002, p. 1–21
[75] OJ L 309, 24.11.2009, p. 1-20
[76] OJ L 271, 18.10.2011, p 1-19
[77] OJ L 196, 21.7.2016, p. 3–43
[78] OJ L 185, 15.7.2011, p. 1–29
[79] OJ L 96, 31.3.2004, p. 20–25
[80] OJ L 122, 24.4.2014, p. 18–43
[81] OJ L 23, 27.1.2010, p. 6–27
[82] https://www.enisa.europa.eu/publications/securing-smart-airports

2. Land Transport (Rail & Road transport)

- **EU/International regulatory and policy environment**

The state of play as regards a comprehensive cyber-security strategy for land transport is far less mature in comparison with the aviation and maritime sectors. There is no effective formal international forum (comparable to ICAO or IMO) leading discussion on land transport security including cyber-security issues. The EU does not have a specific competence on rail cyber security other than that referred to in the NIS Directive.

Land transport covers a range of modes of transport that includes passenger transport by rail, public and urban transport, private vehicles and also freight transport by both road and rail. It is therefore not a homogenous sector and the different forms of transport can have differing security issues and needs which will require some tailoring of the likely solutions.

There are two main challenges for the sector: avoiding the interruption of transport itself in order to assure the flow of freight and passengers and avoiding those transport systems themselves being used as a means for harming people. Additionally, transport operators are very concerned with the risk of financial loss from cyber-attacks, whether this is from hacking with accompanying ransom demands or from fraud targeting revenue transfer systems.

- **Specific issues**

- **Moving from legacy to internet linked systems**
  The rail and public transport sector is increasingly moving from a pre-internet standalone era of control systems that manage the infrastructure (e.g. signalling developments such as ERTMS and train speed control) to one which is highly connected and dependent on connected technology and internet, in some cases wireless, based communications which significantly increases the potential risks of an incident occurring.

20.

21. There is a risk that such safety critical systems could be the target of jamming or spoofing attacks or remotely taken control of by external parties with the intent of directly causing damage, harm to travellers or for demanding a ransom payment from the operator.

22.

23. Road vehicles and road infrastructure are also developing to become cooperative, connected and highly automated systems. Connectivity is technically known as "Cooperative Intelligent Transport Systems (C-ITS)", which are a group of technologies and applications that enable effective data exchange through wireless technologies, allowing vehicles to become connected with each other, with the road infrastructure and with other road users, including vulnerable road users such as pedestrians, cyclists or motorcyclists.

24.

25. The cyber-security of upcoming vehicle-to-vehicle and vehicle-to-infrastructure communications in terms of C-ITS services is critical, and requires action at European level. Without clear rules, adopted at the Union level, C-ITS deployment in the EU will be delayed as investors are looking for a common approach for the internal market.

26.

- **Disruption of communications**
  Although railway systems are designed according to a fail-safe approach, interruption of signals would lead to train stops, but the failure of communications with the train would increase the vulnerability of the system and ability to manage an incident.

27.

- **Cyber-interoperability**
  As the EU develops the single European railway area, it is important that all elements of the network move towards interoperability underpinned by common certification systems. However the development of national cyber security strategies and solutions which are not coordinated at the European level increase the risk of the creation of new barriers being put in place. Also in the case of C-ITS, fragmented security solutions will put interoperability and the safety of end-users at risk.

28.

- **Staff Expertise**
  There is a general lack of expertise of people who both understand traditional security issues and how to manage them and more specific IT knowledge needed to really understand cyber risks for which they are also responsible.

- **Fraud**
  Transport companies are concerned about increasing amounts of fraud being committed by the use of cyber-attacks against their revenue systems.

29.

➢ **Relevant EU Institutions and other actors**

The **European Commission** works together with Member States and stakeholders in addressing a vast array of transport policies. Cyber security and cyber resilience in different modes of transport is an emerging issue.

The principal forum for discussing and collaborating on these issues is through the Commission's **Land Transport Security Experts Group (LANDSEC),** which assists in formulating and implementing the European Union's activities aimed at developing security policy for land transport. Member States and transport sector stakeholders have voiced their concern about the risk of a harmful attack on the IT systems of the European rail industry. The Group regularly discusses sector and national approaches to cybersecurity amongst the full range of security issues that affect land transport systems.

The Commission commissioned a study for the LANDSEC group which developed guidelines on managing cyber risks for SCADA control systems, data flows in container transport and the outsourcing of IT services. The guidelines were shared with LANDSEC group members in early 2016 via the group's online web-portal (accessible by Member State representatives).

Since October 2014, the Commission has also been working to define clear and common rules on Intelligent Transport, including a common security and certificate policy, allowing for interoperability. In order to enable secure, interoperable and safe operation of C-ITS in Europe, the Commission has adopted the **European strategy on Cooperative Intelligent Transport Systems**[2]. This communication includes specific actions on the topic of cyber security. In particular, as announced in the strategy, the Commission is currently working on a delegated act on C-ITS under the **ITS Directive 2010/40/EU**[3] and on guidance documents regarding the European C-ITS security and certificate policy, which are expected to be published already in 2017.

➢ **Relevant Agencies, Key external EU actors and International Organisations**

[2] COM(2016) 766 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0766&from=EN

[3] EC, "Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport", 2010.

The **European Union Agency for Railways** (ERA)[83] is the agency of the European Union (EU) that develops mandatory requirements for European railways and manufacturers in the form of Technical Specifications for Interoperability (TSI). The adoption of a TSI falls into Commission competence. Through the development of technical safety and interoperability standards, the Agency contributes to the implementation of European Union legislation and monitors and disseminates best practices to ensure the interoperability of the rail system. ERA is developing a common approach to safety on the European railway system and contributing to creating a Single European Railway Area without frontiers guaranteeing a high level of safety. While the mandate of ERA does not include security, it can assess the safety consequences that could follow from a security threat.

ENISA has created an expert group to cover security and resilience of Intelligent Public Transports in the context of Smart Cities with the aim of contributing to relevant position and policy papers on security topics and to exchange knowledge in the domain of Intelligent Public Transports. It also published two studies in 2016 that set out good cyber security practices of Intelligent Public Transport operators within the context of smart cities[84] and recommend security measures that could be deployed to protect critical assets of Intelligent Public Transport systems[85].

The Shift2Rail Joint Undertaking has identified cyber-security within its Strategic Master Plan as a priority research and innovation activity, specifically in the area of Advanced Traffic Management and Control Systems and has an objective to establish a network of Railway Cyber Security Experts.

The railway sector differs in its capabilities in dealing with this issue and is dependent to an extent on the significant differences in both the understanding of and the development of capabilities to manage the cyber security risk across the 28 Member States. However some key railway bodies have been active in developing security guidelines for their members i.e. UIC for railway sector and UITP for urban public transport.

3. Maritime Transport

- **Key highlights for the maritime sector**

Maritime cyber security awareness is probably not as advanced , as in the civil aviation sector. It is necessary to undertake and support targeted maritime sector awareness, reinforcing the dialogue with the Shipping industry and the Member States, raising campaigns and cyber security training of shipping companies, port authorities, national authorities including cyber security offices, flag states, etc.

Due to the high ICT complexity, it is major challenge to ensure adequate maritime cyber security. A common strategy and development of good practices for the technology development and implementation of ICT systems would therefore ensure "security by design" for all critical maritime ICT components.

As current regulatory or best practices initiatives and developments are mainly taking place at international level (IMO and industry/international associations) and focusing mainly on the ships side, further efforts should be deployed in relation to the cyber-security developments from the (port) infrastructure side.

As maritime governance is conducted and enforced at different levels (i.e. international, European, national, other), the International Maritime Organization together with the EU Commission and the Member States are strengthening their efforts in order to progress

[83] www.era.europa.eu/
[84] https://www.enisa.europa.eu/publications/smart-cities-architecture-model
[85] https://www.enisa.europa.eu/publications/good-practices-recommendations

on the cyber-security file (to protect ships as well as infrastructure side), in an effort also to align international and EU policies and initiatives in this sector[86].

- **Relevant EU Institutions and other actors**

As part of its activities in the area of transport, the **European Commission** develops policies in the transport security field. In this context, it is leading a number of initiatives regarding cybersecurity in the transport sector, including maritime.

- **Maritime Security** (MARSEC Committee)**, Stakeholders Advisory Group on maritime security (**SAGMAS)

For Maritime, the Commission conducts a regular dialogue with the Member States and Stakeholders in the field of maritime security, through the MARSEC Committee and SAGMAS meetings respectively, where cyber-security issues are also discussed and views and experiences exchanged.

- **EU/International regulatory and policy environment**

In the maritime transport, cybersecurity is starting to grow momentum but remains less advanced than in aviation. The first main initiatives have been taken by industry at a global level notably through its main associations BIMCO, ICS-International Chamber of Shipping[87], by developing for example voluntary Guidelines[88] to help the industry to handle or be prepared for cyber-security threats or how to react to incidents and attacks.

At the international level the 2002 IMO International Ship and Port Facility Security Code (ISPS Code) includes requirements covering the cyber-security dimension of ships.

The IMO guidance document focuses on shipping only, and does not bring ports into the picture, beyond what is the simple ship/port interface, and without entering into the port area, from an infrastructure approach and dimension. This is then an important area (port infrastructure) where developments on cyber-security at global/IMO level are not occurring in parallel with shipping and in which the Commission would like to move forward on as well, with a possible EU initiative.

The Commission is keen to drive this issue forward and as such would already like to base its work in the field on what has been discussed in the IMO and with Industry too. The documents already produced should be used as the basis and foundation of work to be done in the Commission.

[86] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/dependencies-of-maritime-transport-to-icts

[87] notably through its main associations BIMCO, ICS-International Chamber of Shipping

[88] https://ec.europa.eu/maritimeaffairs/policy_en

C. FINANCE AND BANKING SECTORS

This section focuses on the Finance and Banking sectors which are jointly presented. Finance is considered to include traditional financial institutions (e.g. depository, contractual – insurance companies and pension funds - and investment institutions and FMIs) as well as payment services, which may extend beyond banking.

➢ Key highlights for the Finance and Banking sector

The Finance and Banking sector is among the most mature sectors of Operators of Essential Services as defined in the NIS Directive in terms of cybersecurity practices. Cybersecurity is a key concern and security and operational risk and resilience are an integral part of European Commission's DG FISMA's ongoing discussions with the financial sector, national and international regulators. The sector exhibits the following opportunities and challenges in relation to the implementation of the NIS Directive:

Opportunities:

- Improve information sharing on cybersecurity incidents between public and private organisations, as well as between private entities.
- Improve/increase governmental support to financial services cybersecurity and resilience through national, sectorial or European-level CSIRTs and ISACs.
- Harmonization of cybersecurity leading-practices and incident reporting procedures across the EU; possibly also across related regulatory requirements (NIS, GDPR, etc.).
- Increased collaboration among EU institutions and authorities on cyber-security related matters: in defining the strategy, requirements and interdependencies.
- Collaboration with other regulators from other sectors: (a) with sectors on which the financial services industry relies on (e.g. telecommunications, energy etc.), and (b) authorities supervising regulation impacting directly or indirectly the cyber-security requirements, e.g. data protection.

Challenges:

- Increased regulatory complexity and uncertainty regarding legislation applicable and/or implementation and enforcement.
- Partial coverage of the financial sector by the NIS (only credit institutions, trading venues and central clearing parties) and application of lex specialis requirements. Other financial sectors (e.g. payments, insurance, asset management, …) fall outside scope of NIS.
- Renewed regulatory and oversight fragmentation of financial services sectors due to national approaches in cybersecurity.
- Fragmentation and divergence in security requirements at national, EU and/or international level
- Double-reporting of incidents to a variety of competent authorities possibly in different formats and under different thresholds of significance
- Limited buy-in at Board and senior management level of the importance of the cyber-security issues both at the supervised entities and at the regulators / supervisory authorities.

➢ Relevant EU Institutions /bodies

- The **Directorate-General for Financial Stability, Financial Services and Capital Markets Union** (**DG FISMA**)[89] is a Directorate-General of the European

[89] http://ec.europa.eu/dgs/finance/

Commission charged with initiating and implementing EU policy in the area of financial services, including Banking and Finance. As such, DG FISMA is also tasked with sector-specific legislative initiatives regarding or including cybersecurity. Specifically, DG FISMA works on payment security and on the implementation on the financial acquis, which also covers other cyber-security aspects strictly related to financial services.

➢ **Relevant Agencies, Key external EU actors and International Organisations**

- The **European Banking Authority** (EBA)[90] advises both the Financial Institutions but also t he legislative authorities (e.g. DG FISMA) and is mandated to assess risks and vulnerabilities in the banking sector which could include cyber security.

- The **European Central Bank** (ECB)[91] as operator and overseer of key financial market infrastructures and via the **Single Supervisory Mechanism** (SSM)[92] has a supervisory role regarding the financial stability for all the banks subject to the Single Supervisory Mechanism; While cybersecurity is not mandated per se, it be considered an implicit part of the mandate within the context of operational risk.

- The **European Securities and Markets Authority** (ESMA)[93]is an independent EU authority whose purpose is to improve investor protection and promote stable, orderly financial markets. In this context, ESMA identifies cyber-attacks as a key risk in the Joint Committee Report on Risks and Vulnerabilities in the EU Financial System[94].

  The **European Insurance and Occupational Pensions Authority** (EIOPA)[95] is a European Union financial regulatory institution whose core responsibilities are to support the stability of the financial system, transparency of markets and financial products as well as the protection of policyholders, pension scheme members and beneficiaries. In its Financial Stability Report of June 2016[96], EIOPA addresses the increasing exposure of companies to cyber risk.

➢ **Key agencies and organisations at EU level**

- **The European Financial Institutes – Information Sharing and Analysis Centre** (FI-ISAC)**[97]**, is an independent organisation. ENISA initiated a multi-stakeholder discussion on setting up a European ISAC for the financial sector in 2008, and have contributed to this initiative growth and development ever since. The mission of the European FI-ISAC is information exchange on e-channel, cards, central systems and all ICT related topics including cyber-criminal activity affecting the financial community, vulnerabilities, technology, trends, threats, incidents and case-studies. This information exchange helps each member and the banks in the Member States, to raise awareness on potentials risks, and provides an early warning on new threats and vulnerabilities. Membership consists of country representatives coming from the financial sector, national CSIRT's and Law Enforcement Agencies. Other organisations represented are

[90] https://www.eba.europa.eu/
[91] www.ecb.europa.eu/
[92] http://ec.europa.eu/finance/general-policy/banking-union/single-supervisory-mechanism/index_en.htm
[93] https://europa.eu/european-union/about-eu/agencies/esma_en
[94] https://www.esma.europa.eu/sites/default/files/library/2015/11/jc_2015_007_jc_report_on_risks_and_vulnerabilities_in_the_eu_financial_system.pdf
[95] https://eiopa.europa.eu/
[96] https://eiopa.europa.eu/Publications/Reports/Financial_Stability_Report_June_2016.pdf
[97] https://www.fsisac.com/

ENISA, Europol, the ECB, the European Payments Council (EPC) and the European Commission.

- **FS-ISAC should also be mentioned (is international but has a European chapter)**

30.

➢ **Key agencies and Organisations at International level**

- The **Bank for International Settlements** (BIS)[98] is an international financial institution owned by central banks which fosters international monetary and financial cooperation and serves as a bank for central banks. It hosts the Basel Committee for Banking Supervision (BCBS) and the Committee on Payments and Market Infrastructures (CPMI):
- The **Basel Committee on Banking Supervision** (BCBS) is a committee of banking supervisory authorities that provides a forum for regular cooperation on banking supervisory matters. Its objective is to enhance understanding of key supervisory issues and improve the quality of banking supervision worldwide.
- The **Committee on Payments and Market Infrastructures** (CPMI)[99] promotes the safety and efficiency of payment, clearing, settlement and related arrangements, thereby supporting financial stability and the wider economy.

- The **International Organization of Securities Commissions** (IOSCO)[100] is an association of organisations that regulate the world's securities and futures markets.
- The International Association of Insurance supervisors performs a similar role for the insurance sector.

31.

- The **G7 Finance Ministers and Central Bank Governors expert group on cybersecurity** was launched by the G7 Leaders to enhance policy coordination and practical cooperation to promote security and stability in cyberspace[101].

- The **Basel Committee on Banking Supervision** (BCBS)[102] is a committee of banking supervisory authorities that provides a forum for regular cooperation on banking supervisory matters. Its objective is to enhance understanding of key supervisory issues and improve the quality of banking supervision worldwide.

- The **Financial Stability Board** (FSB)[103] is an international body that monitors and makes recommendations about the global financial system within the G20 context. The FSB promotes international financial stability by coordinating national financial authorities and international standard-setting bodies as they work toward developing strong regulatory, supervisory and other financial sector policies.

32.

➢ **EU/international regulatory and policy environment**

The current and evolving regulatory requirement is predominantly characterised by the complexity and uncertainty regarding legislation applicable and/or implementation and enforcement. Specifically, there are two key factors that should be addressed:

[98] https://www.bis.org/
[99] https://www.bis.org/cpmi/
[100] https://www.iosco.org/
[101] http://researchcenter.paloaltonetworks.com/2016/05/cso-in-2016-g7-makes-cybersecurity-a-priority-and-paves-the-way-for-track-1-5-multi-stakeholder-discussions/
[102] https://www.bis.org/bcbs/
[103] http://www.fsb.org/

- Double-reporting of incidents to a variety of competent authorities possibly in different formats and under different thresholds of significance;

- Ambiguity in how the NIS Directive and PSD2 – which is intended to serve as *Lex Specialis* for the payment services, superseding the NIS Directive – and GDPR will apply in practice, i.e. what the final reporting landscape would look like for organisations that must report incidents under either framework.

At the regulatory level, several EU legislative initiatives in the Finance and Banking services sector implicitly relate to cybersecurity requirements, even though such requirements may not be explicitly mentioned. Examples of this include:

- **Directive EU/2015/2366** on payment services in the internal market (**PSD2**) addresses secure communication, secure customer authentication and incident reporting jointly to EBA and ECB. ENISA is mentioned as an advisor to EBA and ECB in Articles 95 & 96 of the PSD2. PSD2 foresees that Financial Institutions are obliged to report cybersecurity incidents to the assigned National Authority, which in turn reports the incident to the EBA and the ECB, who facilitate information sharing among the Member States if needed. In fact, information sharing is mandated in PSD2 between the National Competent Authorities and EBA/ECB.

- The **Central Securities Depositories** (**CSD**) **Regulation** (Article 45) which states the need for CSDs to apply appropriate IT tools in order to identify, monitor and manage sources of operational risk, both internal and external;

- The **European Markets Infrastructure Regulation (EMIR)** and the Commission Delegated Regulation 153/2013 (Article 9) which contain provisions on the need for central counterparties (CCPs) to maintain adequate IT systems for dealing with the complexity of services provided and to ensure high standards of security and confidentiality of the information they hold;

- The **Capital Requirements Regulation** (Regulation 2013/575/EU on Prudential Requirements for Credit Institutions and Investment Firms) and the **Capital Requirements Directive** (Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms) (**CRR/CRD IV**) whose operational risk requirements for financial institutions are relevant to IT-related risks, and are complemented with 'soft law' (e.g. guidelines) issued by the EBA;

- Article 16 of the **Markets in Financial Instruments Directive** (**MiFID**) which requires investment firms to 'have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment, effective control and safeguard arrangements for information processing systems (Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU);

- The **Solvency II Directive** which contains provisions on the specification of the operational risk module of the standard formula; Article 107 of Solvency II sets out capital requirements for operational risk for insurance and reinsurance undertakings, which also includes risks from IT incidents and cyber-attacks;

- **Regulation 909/2014** on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012;

- **Directive 2013/34/EU** of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC;

- **Regulation (EC) No 462/2013** Of the European Parliament and of the Council of 21 May 2013 amending Regulation (EC) No 1060/2009 on credit rating agencies;

- Commission **Delegated Regulation (EU) No. 449/2012** of 21 March 2012 supplementing Regulation **(EC) No 1060/2009** of the European Parliament and of the Council with regard to regulatory technical standards on information for registration and certification of credit rating agencies;

- International level (regulatory example/brief explanation about what it is) and how it links with the European context.

At a policy level, DG FISMA addresses security and operational risk and resilience are an integral part of their ongoing discussions with the financial sector, national and international regulators. Among DG FISMA's ongoing activities in terms of policy are the following:

- Commission Fintech Taskforce work stream on cybersecurity and operational risk
- DG FISMA is involved in the work of Financial Services Committee
- Payment Services Directive II implementation

The EBA's policy activities in this sector include the following:

- The EBA published and submitted to the Commission its final draft Regulatory Technical Standards specifying the Advanced Management Approach in December 2015 (EBA/RTS/2015/02).
- EBA Guidelines on the security of internet payments
- EBA security-related mandates under PSD2, including Guidelines on incident reporting under PSD2, RTS on strong authentication and secure communication, Guidelines on Operational Risk & Security Measures and Opinion on use of Cloud services in the banking sector
- EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP) – consultation paper published

ENISA's activities, publications and recommendations in the domain include, among others:

- Guidelines for security in Mobile Payments and Digital Wallets
- Guidelines for secure use of cloud computing in the Finance Sector
- Network and Information Security in the Finance Sector - comparative analysis across Member States
- Security of blockchain
- Ongoing reports (to be delivered in 2017) on the recommendations and support for the implementation of the NIS Directive, including the finance and banking sector

CPMI/IOSCO are also active in the Guidelines and regulatory technical standards for the sector:

- CPMI-IOSCO Principles for FMIs

33. CPMI-IOSCO Cyber resilience guidance for FMIs

D. HEALTH SECTOR

- **Key highlights for the Health sector**

Overall, the level of cybersecurity maturity in the health sector is lower than that of other sectors as the topic has only in recent years started to get significant traction beyond the Data Protection aspects. The NIS Directive is the first legislative initiative to establish a specific regulatory environment for cybersecurity in the Health sector.

The cybersecurity challenge in the health sector is amplified by the variety of actors involved in the respective processes (outpatient care providers, inpatient care providers, medical device manufacturers, pharmaceutical industry etc.) and the varying degrees of cybersecurity maturity across the different actor categories.

Due to the heterogeneity and complexity of the health sector and the resulting landscape of cybersecurity considerations, a number of different actors are involved in policy making, each addressing a different facet of cybersecurity in health.

- **Relevant EU Institutions /bodies**

34.

- The **Directorate-General for Health and Food Safety** (**DG SANTE**)[104] has a horizontal role in healthcare for legislative initiatives. Specifically unit B3 on cross-border healthcare and eHealth deals with eHealth related topic in the context of cross-border healthcare. The unit is placing much emphasis on the improvement of eHealth interoperability and standardisation through the building of the eHealth Digital Service Infrastructure (eHDSI). The eHDSI allows Member States to exchange health data (ePrescriptions and Patient Summaries) with other Member States.

- **The Directorate-General for** Communications Networks, Content & Technology (**DG Connect)** has established a specific Unit for eHealth within the Digital Society, Trust and Cyber Security Directorate, namely the **e-Health, Well-being, and Ageing Unit** (**Unit H.3**). Unit H.3 leads the Mobile Health (mHealth)[105] initiative as a sub-segment of eHealth which covers medical and public health practice supported by mobile devices. It especially includes the use of mobile communication devices for health and well-being services and information purposes as well as mobile health applications.

- The **Directorate-General for the Internal Market, Industry, Entrepreneurship and SMEs** (**DG GROWTH**) leads legislative initiatives regarding the medical devices aspect of healthcare[106] within the context of its SME initiatives related to the industry for medical devices, where cybersecurity of these devices is identified as a key aspect.

35.

- **Relevant Agencies, Key external EU actors and International Organisations**

36.

- In accordance with the Cross-border Healthcare Directive (2011/24/eu), DG SANTE has created and is managing the **eHealth Network**[107], a voluntary network of Member State representatives dealing with eHealth in the EU. The

[104] http://ec.europa.eu/dgs/health_food-safety/index_en.htm
[105] https://ec.europa.eu/digital-single-market/en/mhealth
[106] https://ec.europa.eu/growth/sectors/medical-devices_en
[107] http://ec.europa.eu/health/ehealth/policy/network/index_en.htm

eHealth Network's activities are related to strategic aspects concerning eHealth. The Cross border healthcare and eHealth Unit of DG SANTE provide the secretariat, supported by e-Health, Well-being, and Ageing Unit of DG CNECT.

- **JAseHN**[108] or the **Joint Action supporting the eHealth Network** serves as the main preparatory body for the eHealth Network to develop political recommendations and other instruments for cooperation in the four specific priority areas that are defined in the eHealth Network's Multiannual Work Plan (MWP) 2015-2018, namely interoperability and standardization, monitoring and assessment of implementation, exchange of knowledge and global cooperation and positioning.

37.

- **EU regulatory and policy environment**

There is no significantly developed regulatory framework when it comes to cybersecurity in the Health sector. Data Protection is traditionally considered to be of great importance for electronic patient and health data so the **Data Protection Directive 95/46/EC**[109] and its successor the new **General Data Protection Regulation** (**GDPR**)[110] are of particular relevance.

The main regulatory framework on which eHealth is based is the **Directive 2011/24/eu**[111] **on the application of patients' rights in cross-border healthcare**. Cybersecurity is however not included for consideration in this Directive.

The Commission has published a Staff Working Document[112] on the existing EU legal framework applicable to lifestyle and wellbeing apps, providing legal guidance on EU legislation in the field to app developers, medical device manufacturers, digital distribution platforms, etc. Other European mHealth initiatives include the **Privacy Code of Conduct for mHealth apps**[113], led by the EC based on the 2014 Green paper on mHealth[114], with the support of industry and based on the GDPR which covers the topics of privacy and security in mHealth apps and the **mHealth assessment guidelines working group**[115], comprising representatives of patients, health professionals and providers, payers, industry, academia and public authorities which is appointed to provide common quality criteria and assessment methodologies that could help different stakeholders, in particular end-users, in assessing the validity and reliability of mobile health applications.

A new **Medical Devices Regulation** (MDR)[116] is currently under evaluation to replace the existing Medical Device Directive[117] (Council Directive 93/42/EEC of 14 June 1993) concerning medical devices. The MDR will include specific cybersecurity requirements for medical device manufacturers.

ENISA's activities, publications and recommendations in the domain include, among others:

- Report on Security and Resilience in eHealth Infrastructures and Services[118]
- Report on Cyber security and resilience for Smart Hospitals[119]

---

108 http://jasehn.eu/
109 http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:31995L0046
110 http://ec.europa.eu/justice/data-protection/reform/index_en.htm
111 http://data.europa.eu/eli/dir/2011/24/oj
112 https://ec.europa.eu/digital-single-market/en/news/commission-staff-working-document-existing-eu-legal-framework-applicable-lifestyle-and
113 https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps
114 https://ec.europa.eu/digital-single-market/en/news/green-paper-mobile-health-mhealth
115 https://ec.europa.eu/digital-single-market/en/news/new-eu-working-group-aims-draft-guidelines-improve-mhealth-apps-data-quality
116 http://data.consilium.europa.eu/doc/document/ST-11662-2016-INIT/en/pdf
117 https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/medical-devices_en
118 https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services

- Report of Cloud Security for eHealth (to be delivered in 2017)
- Self-assessment cybersecurity maturity questionnaire for Healthcare Organisations (to be delivered in 2017)
- Ongoing reports (to be delivered in 2017) on the recommendations and support for the implementation of the NIS Directive, including the Health sector

38.

[119] https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

E. DRINKING WATER SECTOR

The present section focuses on cybersecurity issues in Sector 6 of Annex II, namely Drinking Water Supply and Distribution.

➢ Key highlights for the Drinking Water Sector

The key challenge for the drinking water sector in terms of cybersecurity is the risk of possible malicious contamination of drinking water with chemicals. A further concern is the security of supply, meaning that the drinking water distribution could be interrupted by cyberattacks on control systems, pumps, etc.

➢ Relevant EU Institutions /bodies

- The European Commission's DG ENVIRONMENT (Unit C2) is responsible for the Drinking Water Directive (DWD) 98/83/EC[120]. Please note that the implementation in Member States is almost exclusively done by the Ministries of Health.

- An Expert Group is established under the Directive to provide advice and expertise to the Commission and its services in relation to its implementation. The Group meets every 6-9 months. Documents are available on CIRCABC[121].

- Security issues are also tackled by the European Reference Network for Critical Infrastructure Protection (ERNCIP), Thematic Group Drinking Water, run by the Joint Research Center[122] .

39.

➢ EU/international regulatory and policy environment

- DWD regulates the quality of drinking water (drinking water safety), but not its supply. It does not address security or emergency issues[123].

- The directive puts an obligation to inform consumers and to prohibit or restrict the supply if drinking water constitutes a potential danger to human health. The Directive refers to Drinking Water Supplies (= supply zones with uniform water quality). It distinguishes between large supplies > 1000 m3/day (or serving more than 5000 people, ~ 11,000 zones in the EU, reporting obligation to the Commission), and small supplies < 1000 m3/day (~ 85,000 zones in the EU).

- The Drinking Water Directive is currently under Revision. The REFIT Evaluation was completed on 1 December 2016 (SWD (2016)428 final). The revision of DWD was officially included in Commission Work Programme for 2017[124]. Currently, an Impact Assessment is under preparation (proposal scheduled for end 2017).
- There is currently no intention to extend the scope of the Drinking Water legislation towards security/cybersecurity. However, one of the identified changes to the DWD that is currently being analysed in detail is to introduce a risk-based approach and water safety planning. Thereby it should be taken into account that safety planning and security planning have commonalities. The coherence of responsibilities and measures under both Directives should be ensured.

---

[120] http://ec.europa.eu/environment/water/water-drink/index_en.html
[121] https://circabc.europa.eu/w/browse/79c232d0-c393-43f2-a0e2-1244d0380397
[122] https://erncip-project.jrc.ec.europa.eu/networks/tgs/water
[123] ENV-DRINKING-WATER@ec.europa.eu
[124] COM(2016)710 final

- The analogy between 'essential services' and 'very large drinking supplies' should be further analysed as the size of a supply and the number of citizens affected or possibly affected are important factors for the criticality and the risk assessment. Therefore the identification of operators of essential services under the NIS Directive as required under Article 5 of the NIS Directive should take the size and definitions of drinking water supplies/suppliers of the Drinking Water Directive and of a future revision proposal into account.

Annex 10: Who Is Affected by the Initiative and How?

This annex describes the practical implications of the preferred option[125] identified in the Impact Assessment for stakeholder groups likely to be directly or indirectly affected by the initiative.

For each stakeholder group, the relevant impacts of the preferred option will be discussed. Wherever possible, potential costs that may be incurred will be indicated.

Member States

Member States are expected to significantly benefit from the initiative. They could count on long-term support of a reinforced agency focusing on areas where it would bring the most added value: i.e. policy development and implementation; information knowledge and awareness raising; research; operational cooperation and crisis management; market related tasks (certification, standardisation). In particular, as an essential part of its activities to support the internal market, ENISA would support EU policy in the field of ICT security certification, by ensuring an administrative maintenance and technical management of a European ICT security certification framework.

The overall expected impact on Member States would include increased capabilities and preparedness to face cyber threats as well as improved cooperation and coordination across Member States on issues of common interest. This should in turn result in increased cybersecurity resilience across the EU and help build trust in the digital single market. At the same time, the preferred option would leave sufficient room for national actions in sensitive areas such as national security.

More in detail, within Member States, two categories of stakeholders would be in particular impacted by the initiative:

1. National Authorities

They would benefit from various ENISA's products and services, including, among others:

- long-term strategic analyses of cyber threats and incidents helping Member States to identify emerging trends and ways to adapt their cybersecurity efforts;
- EU-wide independent guidance and reports on cybersecurity matters,
- brokerage of expertise and good practices between Member States
- support for review of the national security strategies,
- trainings and training material.

National authorities would be also positively impacted by having ENISA's assistance in the implementation of the NIS Directive and subsequent legislation in cybersecurity. In particular, ENISA's contribution to policy development and implementation in the area of NIS is expected to support cooperation amongst national authorities and regulators across all sectors in the NIS Directive and the telecoms sector to promote best practices and exchange lessons learned amongst sectors.

As far as ICT security certification and labelling is concerned, national authorities would benefit from:

[125] The preferred option is a combination of **Option 2** ('Enhanced ENISA') with regard to **ENISA** and **Option 3** (Establishing a European ICT security certification and labelling framework) for **certification and labelling.**

- technical expertise provided by ENISA
- the establishment of an institutional framework that enables to identify common priority areas for security certification and labelling.

An important impact can be also foreseen for national authorities as buyers of ICT products and services. The promotion of certification and labelling under the Framework, would allow national authorities to make more informed purchase decisions. They could e.g. decide to procure ICT solutions with a certain cybersecurity assurance and, thanks to the mutual recognition system, they would reap the full benefits of unfettered competition and cross-border free trade across the Union.

2. Computer Security Incident Response Teams (CSIRTs)

National CSIRTs have already strong ties with ENISA, which helped nurturing their capabilities and build their community in the EU. They are expected to benefit from the preferred option as the enhanced ENISA would be able to respond to their needs in a more comprehensive way. In particular, the support would be structured linking the key areas of:

- **capacity building** including e.g. trainings, training material, guidance on improving maturity and establishing KPIs,
- **operational cooperation**, including:
    - technical support for back-end services (e.g. information portal that enables CSIRTs to exchange information on best practices and actual incidents and threats and support voluntary cooperation in case of incidents[126]);
    - drafting and updating CSIRT Network Standard Operating Procedures;
    - pan-European cyber exercises;
    - back-end support for analysis of vulnerabilities, artefacts and incidents in cooperation with CERT-EU and
    - crisis management (for instance, in the context of the Cybersecurity Blueprint collect and aggregate national operational reports and produce a common situational awareness report for decision makers in case of large scale cross-border cybersecurity incidents).

It is estimated that the costs of the initiative for Member States would be limited. In particular, most of the expenses would be borne under the EU budget[127] within the Multiannual Financial Framework. Member States could provide voluntary contribution to ENISA (as it is the case today) and would be required to pay fairly small amounts for the maintenance of the European ICT Security Certification Framework[128]. Additional costs could be expected for those national authorities that intend to participate in the development of future European certification schemes within the Framework.

[126] ENISA will host key elements of the Core Service Platform, funded through the CEF programme, which provides the CSIRT Network communication tools and a cooperative environment on which to analyse cybersecurity incidents.
[127] Reference to Annex 6 for the estimates on the costs for ENISA and Annex 7 for the estimates on the costs for the ICT
[128] It is estimated to be approximately EUR 58,000 per year per each Member State.

Businesses

Businesses are expected to be affected by the initiative from different perspectives: as potential victims of cyber incidents, as producers of ICT products (cybersecurity products and/or ICT products that could be certified), as buyers of ICT products. While the changes related to ENISA's mandate are likely to impact businesses across the board, the set-up of the ICT security certification framework impacts in particular the producers and buyers of ICT products and services.

First, the enhanced ENISA would positively impact businesses across different sectors, in particular those operating in critical sectors. A permanent mandate would ensure that ENISA supports businesses in a sustainable manner, providing opportunities both to the Agency and to its constituents for a long term vision and planning of the work. The suggested revision of the Agency's governance, giving more prominent voice to the Permanent Stakeholder Group in defining priorities for the work programme, would allow businesses to receive support better adjusted to their real needs related to increasing cybersecurity capabilities and preparedness. As presented earlier with regard to Member States, businesses would also benefit from the provision of reliable, robust analyses on the threat landscape, incidents and the related existing market solutions as well as from guidance on cyber hygiene that could help better protect their organisations. In particular, the operators of essential services covered by the NIS Directive would benefit from EU-wide good practices, guidelines and recommendations on security measures and incident reporting.

Second, businesses operating in the cybersecurity sector could benefit from the information provided by the Agency's playing the role of a market observatory. ENISA would make available analyses of the main trends in the EU cybersecurity market in order to enhance alignment of the demand and supply sides and thus help enhance the competitiveness of the companies in the sector.

Third, a positive impact can be inferred on the capabilities of private actors, operating within Member States and cross borders, through the contribution of ENISA to the establishment of Information Sharing and Analysis Centres (ISACs) in various sectors. This would include providing best practices and guidance on available tools, procedures as well as appropriately addressing regulatory issues related to information sharing.

Fourth, producers of ICT products that already certify their products and sell them across the EU would be positively impacted by the establishment of the European ICT security certification and labelling framework. The mutual recognition system would allow them to enjoy costs savings by reducing to one the number of certification processes their products need to undergo. The same applies to companies that will be certifying their products in the future. The mutual recognition would also boost the competitiveness of firms operating cross-borders - by providing an incentive to certify their products and thus helping them reap the advantages of increased trust in the digital solutions as well as by gaining access to market segments where certification is required (e.g. some areas of public procurement). As the preferred option is based on voluntary certification and labelling, it would not impose additional costs for producers.

Fifth, the businesses that are buyers of ICT products and services would be positively impacted by the expected increase in the number of certified products/services, stimulated by the policy in this field and the establishment of the framework. This would also increase the amount of available information on the level of assurance of the security properties of products/services and thus increase trust in the digital solutions. In addition, the ICT security certification framework will provide a strong incentive for operators of essential services to require that the products they buy are certified.

Finally, as the ICT security certification framework will provide the possibility for a variety of stakeholders to contribute to future certification activities, industry representatives as well as consumers associations are expected to participate in regular meetings. Such a multi-stakeholder approach would increase transparency and inclusiveness of the process to develop European certification schemes, as well as trust among actors operating in the Digital Single Market.

SMEs

For SMEs and micro-enterprises, the access to free, high quality and independent information, analyses and recommendations provided by the enhanced ENISA can significantly release their budgets, for which investments in cybersecurity can represent a significant burden. This particularly applies to the dissemination of good practices of cyber-hygiene, since this could help limit the overall number of incidents affecting companies, which are currently often due to incorrect human behaviours. However, it has to be noted that the overall positive impact on SMEs and microenterprises might be significantly limited due to the linguistic barriers. Unless the Agency would be able to devote a bigger part of its resources to translation services or national experts cooperating with the agency take on the responsibility for translation, the dissemination of material exclusively in English limits its accessibility throughout the EU.

With regard to certification and labelling, the proposed option would significantly reduce costs and administrative burden for SMEs that already certify (or are willing to certify) their products and services. Even more importantly than in case of big businesses that have usually more resources, the mutual recognition system would allow SMEs to enjoy costs savings by reducing to one the number of certification processes their products need to undergo. It would also eliminate a potential market-entry barrier (for both new business and SMEs) and enable access to a wider cybersecurity market.

EU institutions, Agencies and bodies

The preferred option would positively impact the EU institutions, Agencies and bodies as they could count on an enhanced agency that would better support the EU policy development and implementation, as well as the definition of research priorities on cybersecurity by providing expertise, guidelines and recommendations. This would benefit the institutions, agencies and bodies addressing cybersecurity at both horizontal and sectoral level, including by providing a reference point to ensure coherence between the two.

EU institutions, Agencies and bodies, in their capacity as buyers, would also benefit from the expected increase in the number of certified products and services; and thus from increased information on the level of assurance of the security properties of ICT products and services they procure.

Citizens

A positive, although indirect, impact can be expected on the citizens with regard to their cybersecurity. An enhanced EU agency can contribute to improving cybersecurity resilience, which in turn should increase trust of EU citizens and businesses in the digital society. This is in particular relevant for the protection of citizens' access to essential services, such as energy, healthcare, water, transport, as well as the security of personal data. In addition, the expected increase in the number of certified devices, including consumer goods, could reduce the exposure of citizens to cyber threats.

Furthermore, the preferred option is expected to contribute to raising citizens' awareness of cyber threats and ways to handle them. An enhanced ENISA would engage in a series of activities that are expected to positively impact the overall level of information and knowledge on cyber issues. It would include: the promotion and sharing of best practices from across the EU by pooling information on cybersecurity deriving from the EU and national institutions, agencies and bodies; the provision of advice, guidance and best practices for the cyber hygiene within the organisations; and the regular organisation of awareness raising campaigns in coordination with the responsible authorities in the Member States.

Finally, the promotion of certification and labelling under the ICT security certification Framework, would allow citizens to make more informed purchase decisions related to ICT products and services. This would also enhance a chain of trust among manufacturers and buyers of ICT solutions.

The ICT security certification landscape

International schemes and other initiatives

International Scheme and relevant standards	
Scheme	**Brief Description**
SOG-IS	The Senior Officials Group – Information Systems Security (SOG-IS) agreement was produced in response to the EU Council Decision of March 31st 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC) on common information technology security evaluation criteria. Currently, SOG-IS MRA is the main certification mechanism existing at European level. However, it only includes 12 Member States plus Norway and has developed only a few protection profiles[129] regarding digital products (such as digital tachograph, digital signatures and smart cards).
Common Criteria (also known as ISO 15408)[130].	The Common Criteria for Information Technology Security Evaluation (commonly known as CC) is an international standard (ISO/IEC 15408) for computer security evaluation. It is based on third party evaluation and envisages 7 Evaluation Assurance Levels (EAL). The CC and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that CC certificates are recognized by all the signatories of the CCRA. Within the current version of CCRA only evaluations up to EAL 2 are mutually recognized.
Information Technology Security Evaluation Criteria (ITSEC)	The Information Technology Security Evaluation Criteria (ITSEC) is a structured set of criteria for evaluating computer security within products and systems. It is still used for some evaluation in the classified information but it has to be considered superseded by the publication of ISO 15408 Common Criteria for ICT security product evaluations.
ISA Secure Certification Programme[131].	ISASecure is scheme that 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 government of Japan has adopted ISASecure as part of their critical infrastructure protection scheme and has set up an

[131] http://www.isasecure.org/en-US/

International Scheme and relevant standards	
Scheme	**Brief Description**
	accredited test lab to process certifications locally in Japan.
Federal Information Processing Standards FIPS-140[132].	Federal Information Processing Standards (FIPS) are standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors.
Industrial Automation and Control Systems (ISA/IEC-62443 /IACS)[133].	ISA/IEC-62443 is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). It applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.
EN50128.	It specifies procedures and technical requirements for the development of programmable electronic systems for use in railway control and protection applications
ISO 27001[134].	ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. The ISO 27001 standard provides a framework that helps organisations: protect clients and employee information; manage risks to information security effectively; achieve compliance; protects the company's brand image.
ISO/IEC 19790 and ISO/IEC 24759	ISO/IEC 19790 and ISO/IEC 24759 are applicable to validate whether the cryptographic core of any security product is properly implementing an approved suite of cryptographic protocols, modes of operation and key sizes, while protecting this implementation and the critical security parameters, such as keys, in accordance to the design and specification requirements laid out in the standards. There are four levels of security defined, and ISO/IEC 19790 includes a variety of possible implementations, both software and hardware.
IECEE CB Scheme[135]	It is operated by the IEC System of Conformity Assessment Schemes for Electrotechical Equipment and Components (IECEE), is an international system for mutual acceptance of test reports and certificates dealing with the safety of electrical and electronic components, equipment and products. It is a multilateral agreement among participating countries and certification organizations, which aims to facilitate trade by promoting

[132] http://csrc.nist.gov/groups/STM/cmvp/standards.html
[133] See: https://www.isa.org/isa99/
[134] https://www.iso.org/standard/54534.html.
[135] https://www.iecee.org/about/cb-scheme/.

International Scheme and relevant standards	
Scheme	**Brief Description**
	harmonization of national standards with International Standards and cooperation among accepted National Certification Authorities (NCBs) worldwide.

National Scheme	
Member State	**Brief Description**
France[136]	Certification Sécuritaire de Premier Niveau (CSPN) is an IT Security Certification Scheme established by the National Cybersecurity Agency of France (Agence nationale de la sécurité des systèmes d'information – ANSSI) in 2008. Its main purpose is to offer a faster and cheaper alternative for IT Security Certification as compared to the CC approach. The security criteria, as well as the evaluation methodology and process are based on an ANSSI created standard. The cost of each CSPN certification is in the region of 25.000 – 35.000 euro while duration of process is approximately of 3 months (CC evaluation of a smart card can take from 6 months to 1 year). Yearly, ANSSI receives around 50 submissions for certification under CSPN. It issues around 25 CSPN certificates (mainly on software) and 100 CC certificates (mainly hardware) per year. Currently, ANSSI recognises and issues two main types of labels. These labels are used for: - certifying products - qualifying products and services
Germany[137].	The German Federal Office for Information Security (BSI) is developing an approach for low level assurance to improve the efficiency of Common Criteria evaluation.
UK	The *Commercial Product Assurance* (CPA)[138] is the UK national scheme for commercial off-the-shelf products; products successfully evaluated according to CPA obtain a Foundation Grade certification, meaning that they proved to be good commercial security practice and are suitable for lower threat environments. CPA is open to all vendors, developers and suppliers of security products with a UK sales base. There is no Mutual Recognition Agreement (MRA) for CPA, which means that products tested in the UK will not normally be accepted in other markets. CPA is similar to common criteria, however not so widely recognised outside of UK. Originated in the UK, Cyber Essentials is a government backed cybersecurity scheme designed to guide businesses in protecting themselves against data breaches and cyber threats.originating from the internet aimed at

[136] Based on information from website (http://www.ssi.gouv.fr/administration/produits-certifies/cspn/) and from official case study presentation (ANSSI, 2015).
[137] Based on information reported in the JRC study, Baldini et al. (2017).
[138] https://www.cesg.gov.uk/scheme/commercial-product-assurance-products-foundation-grade

National Scheme	
Member State	**Brief Description**
	an organisation's IT structure. IASME is a UK-based standard for information assurance at small-to-medium enterprises (SMEs). It provides criteria and certification for small-to-medium business cyber security readiness
The Netherlands	The Dutch Baseline Security Product Assessment (BSPA) scheme is intended to judge the suitability of IT security products for use in the "sensitive but unclassified" domain. The BSPA scheme is in pilot phase since 2015. The pilot is expected to end in 2017 and then the scheme will be operational. In the pilot phase 6 requests for certification were received. The average cost of a certification under BSPA is € 40.000. The overall process can take up to 2 months.
Italy	A recent Italian decree (February 2017) promotes the establishment of a national centre for the evaluation and certification of ICT products used in critical infrastructures.
Norway	Norway has intention to develop a protection profile based on Common Criteria.

Annex 12: Case studies

Case Study – "The impact of an EU wide Certification Scheme on the Smart-Meter Industry"

A smart-meter company, which wants to sell its products in two Member States e.g. France and UK.

	Now	Future

Requirements	• *In order to sell in UK and France manufacturers have to certify against different schemes:*
	  ○ *CPA (Commercial Product Assurance) in UK,*
	  ○ *CSPN (Certification de Sécurité de Premier Niveau) in France*
		• Manufacturers will need to undergo a single certification process, as envisaged in the future European certification scheme for smart meters. The resulting certificate will be accepted by all public authorities in Member States.

Cost	• The overall cost is at least 300 thousand euros for the two markets (about 150 thousand euro in UK and about 150 thousand euros in France).	• The estimation of costs saving ranges up **to 80% of current costs**

Time	• **6 to 18 months.** This estimate takes into account:
	  ○ Completion of multiple certifications processes and supporting documentation
	  ○ Identification of various requirements that a vendors needs to comply with.
	  ○ limited number of conformity assessment bodies able to certify against the requirements of different schemes.
		• **Faster process** that takes into account:
		  ○ Role of ENISA that provides information needed for compliance with the European scheme (e.g. specialised conformity assessment; documentation)
		  ○ Completion of single process : no multiple certifications are needed and capacities of existing CABs can be used more efficiently

Other	• **Different methodologies** for risk assessment and definition of security requirements	• **Standard methodologies** for risk assessment and definition of security requirements

Full Description:

Methodology: The research methodology of this case study is based on literature retrieved from desk research and on the analysis of multiple interviews with cybersecurity experts and professionals working in the Smart-Meter industry.

Background: By May 2014, Member States committed to rolling out close to 200 million smart meters for electricity and 45 million for gas by 2020 at a total potential investment of €45 billion. By 2020, it is expected that almost 72% of European consumers will have a smart meter for electricity while 40% will have one for gas. Up to date, 80 million smart meters have been installed in the EU28 and Norway, which constitutes 30% of the overall European electricity metering points[139]. With potentially millions of networked end-points, there are significant cyber threats organizations and consumers will be exposed to.

Fragmentation of the Smart Meter Industry: Various and not fully coordinated certification initiatives across Europe are increasing fragmentation in the domain of ICT certification and therefore also for Smart-Meter industry, resulting in duplication of efforts and waste of resources. The non-exhaustive list of certification schemes applicable to Smart Meters across Europe includes, among others:

- CPA (Commercial Product Assurance) is the certification scheme recognised in UK,
- CSPN (Certification de Sécurité de Premier Niveau) is the certification scheme recognised in France,
- A protection profile based on Common Criteria is the certification scheme recognised by BSI in Germany.

These three European Countries **do not recognise** each other's certification scheme.

The processes of certification are based on national requirements. In the UK, they are called security objectives. Based on these requirements and objectives, each MS has defined a security certification approach at a national level. There is also national communications infrastructure for devices connected to smart-meters, including interfaces with the different stakeholders involved such as the German Smart Meter "**Gateway**" and in the UK the so-called "**Communication Hub**". Other national initiatives are emerging as the **Dutch Smart Meter Requirements** (DSMR) developed by the Dutch national organization of DSO's "Netbeheer Nederland". If Member States across Europe continue not to accept each other's certification schemes, each Member State will continue to improve its own certification scheme and this could create a strong legacy, making harmonisation more difficult. Another problem regards a European agreement on minimum requirements, on documentations and tests results for the same functionality and in the same language, ready and accepted by the different authorities of different countries. Furthermore, such fragmentation is also happening on the evaluation side; the three different certification schemes mentioned above require three different evaluation methodologies and it's not always sure that they give the same results. There are only limited numbers of Conformity Assessment Bodies (CAB) that are able to certify against the requirements of different schemes and the evaluation period for smart meters products, as mentioned above, can usually last from **6 months to 18 months**. In this way, additional market entry barriers are created.

Cost for Certification: The proliferation of national certification schemes increases the costs for businesses operating cross-border and is likely to create obstacles for the internal market, as it raises the costs for companies/vendors operating across borders. This barrier is more significant for small and medium sized enterprises, which usually have less resources to dedicate to certification programmes.

To provide a concrete example, considering that the cost of certification depends on products, evaluation assurance level needed or components to be evaluated, the cost of certification can reach up to more than 1 million euros and the SMEs are out of this gain. For BSI "**Smart Meter Gateway**" certificate the cost is much more than **one million euros**. The cost for smart meters certification in

[139] USmartConsumer Project, European Smart Metering Landscape Report, "Utilities and consumers", 2016

UK is almost **150 thousand euro**. In France, the cost it is similar to the UK, about **150 thousand euros or more.** In the Netherlands, the average costs of a certification under Baseline Security Product Assessment (BSPA) scheme are approximately **40 thousand euros**. The significant difference of costs for certification between Germany and other Member States have various reasons. France is for instance more focused on testing in a fixed time; i.e. given a fixed time the device has to pass all the security tests during that time. At the end of the fixed time, a final report is sent on whether it is working fine or not. The German approach has a higher level of tests and assurance. On the other hand in the UK and in France a security assessment is performed on one product, while in Germany the whole infrastructure needs to be tested and certified. Considering that these national certification schemes are not mutually recognised, smart metering companies should sustain additional costs in order to enter another Member State's market. In fact, the total cost for certification usually ranges **from 150 thousand euros to 1 million euros and more.** Only one of the biggest smart-metering companies is starting a certification to enter other markets and all the other companies are present only in the German market. In this context, one of the most important barriers to trade for the smart metering industry is the costs for certification. In the absence of an EU wide certification framework a smart metering company that wants to access the French market must certificate its products under the CSPN scheme and once again under the CPA scheme to enter the UK market, therefore it would pay **300 thousand euros**. With an EU wide framework, as the product certification of France deemed as equivalent to the one in the UK, the smart-meter company will have to certificate only once but will access the French and English market paying a cost of around 150 thousand euros and a **direct saving of 150 thousand euros**. More in general, it is estimated that the introduction of an EU wide certification framework could lead to smart meters companies **saving up to 80% on costs.**

Benefits for the Smart Meter Industry of an EU wide Certification Framework: For the smart-meters industry a European scheme would be a valuable policy option. It would make certification schemes mutually recognised across Europe, and standardise a methodology on how risks are assessed and how security requirements are defined. Moreover, it would be very important to have flexibility in certification scheme, determined also by the risk connected to the product evaluated and the risk connected to the location of the product. The introduction of an EU wide certification scheme will produce many benefits for the smart meters industry including:

- The reduction of fragmentation;
- The reduction of market barriers; and
- The reduction of the costs for certification.

Conclusion: There is no common baseline set of security requirements that can be recognized by all participating EU Member States. At least three Member States have defined their own protection profiles. These requirements are different per country, based on different standards and adopted by technical committees. There is no scheme that includes all aspects and enables a pan European approach[140]. In order to improve the current situation and to reduce the market fragmentation and the costs for certification, the introduction of an EU wide certification scheme could have a positive impact for the smart meter industry. A European framework would also reduce the information asymmetry on security requirements of ICT products and make the European market less fragmented.

[140] ENISA, Smart grid security certification in Europe, December 2014

Case Study – "The impact of an EU wide Certification Scheme on Cloud Computing Industry"

	Now	Future
Requirements	• In order to sell Cloud Computing Products / Services in France and Germany providers have to certify against: *SecNumCloud* **and** *Compliance Controls Catalogue (C5)*	• Providers need to undergo a single certification process, as envisaged in the future European certification scheme for cloud computing. The resulting certificate will be accepted by all public authorities in Member States
Cost	• Costs associated to compliance with different technical rules and multiple testing is estimated around 1.2 billion euro, that accounts for **2% to 10%** of companies' annual expenditures.	• An increased level of competition, introducing an EU wide Certification Scheme, would result in a **yearly saving of € 1.1 billion in the EU public sector alone**
Time	• **Around 7-9 months** due to the multiple audit and testing processes to obtain several certifications	• **Reduced time**: duration of a single process is estimated to take around 4 to 6 months. ENISA would accelerate the process by providing the information needed for compliance with the European scheme
Other	• Faced with co-existence of multiple schemes and standards[141], end-users (esp. in the banking sector) are not able to compare and judge which scheme or standard would best satisfy their particular security requirements. This deteriorates the trust in cloud computing services.	• The existence of a security certification scheme for cloud computing agreed at EU level, increases the trust in this service • Competitive gain for cloud providers due to cost and time reduction

[141] ECSO has published a State-of-the-Art Syllabus listing 8 different schemes and standards to certify the security of cloud computing services. See here: www.upm.es/observatorio/vi/gestor_general/recuperar_archivo.jsp?idf=642&tipo=2

Full Description:

Methodology: This case study is based on information obtained from secondary sources (literature review), from the analysis of the European landscape of cloud computing industry conducted on the basis of an online search and from interviews conducted with different impacted stakeholders.

Background: The ongoing digital transformation is strategically affecting both private and public sector organisations also in terms of cybersecurity[142]. Cloud computing has the potential to reduce IT expenditure and boost organisational flexibility while at the same time improving the scope for delivering flexible high-quality new services. Some of the general benefits are reducing costs, increasing the storage capabilities and the chance to adapt in a flexible way to the changing business conditions[143]. These benefits can be applied in a lot of different domains and fields.

The increase in the use of cloud globally is also visible from the market, over the last two years[144]. In 2017, spending on public cloud infrastructure as a service hardware and software is forecast to reach **61 billion U.S. dollars worldwide**[145]. According to Gartner, Inc., the highest growth will come from cloud system infrastructure services (IaaS), which is projected to grow **36.8 percent in 2017 to reach $34.6 billion**. Cloud application services (SaaS) is expected to grow 20.1 percent to reach $46.3 billion[146].

Despite its growing influence, concerns regarding cloud computing still remain. There are in fact challenges that it still has to face, such as: **data protection, data recovery and availability, management capabilities and regulatory and compliance restrictions**[147].

Incidents related to cloud computing services worry the companies especially for sectors such as finance where a data breach can cause huge economic and reputable damages. According to representatives from European banks, they are not very sure if the data are stored in a secure way, especially according to the various jurisdictions of different countries.

Cloud computing is going to be fundamental for the future. For this reason, it is necessary that it as secure as possible.

Fragmentation of the Cloud Computing Industry: Cloud service providers offer their services internationally in several markets. Therefore, national approaches for certification and assurance are of limited use to them. National cyber security authorities can usually only set national standards, even if other countries use them too[148]. ANSSI (Agence national de la sécurité des systèmes d'information) and the BSI have been very intensively involved with the security of cloud computing in recent years. Both authorities arrived at a very similar understanding of the cloud security standards that need to be met, and both initiated new ways of verifying secure cloud computing, since the existing certifications failed to adequately meet the needs in this area. However, both authorities pursued different paths[149].

- **Compliance Controls Catalogue (C5)** - The BSI developed the Cloud Computing Compliance Controls Catalogue (C5). This catalogue, which is closely oriented to tried and tested standards, defines the requirements for the secure provision of services critical to businesses, which the cloud provider must meet. Additionally, the provider must make their offer transparent, such as the location of data processing and the subcontractor. The auditing process is conducted in line with the international recognised standard, the ISAE 3000. The audit report is based on standards such as the ISAE 3402 and SOC 2. Auditors and cloud experts conduct this audit and issue an audit opinion, for which the auditor bears liability. The C5 also contains standards for greater protection needs and can be individually extended – for example for a specific industrial sector. The BSI sets the standards and specifies criteria for the audit, but has no further supervisory role with regard to specific procedures.

---

142 https://www.enisa.europa.eu/publications/exploring-cloud-incidents
143 http://picse.eu/sites/default/files/ProcuringCloudServicesToday_March2016_web.pdf
144 https://www.forbes.com/sites/louiscolumbus/2016/03/13/roundup-of-cloud-computing-forecasts-and-market-estimates-2016/#51dfa21b2187
145 https://www.statista.com/statistics/507952/worldwide-public-cloud-infrastructure-hardware-and-software-spending-by-segment/
146 http://www.gartner.com/newsroom/id/3616417
147 http://www.thbs.com/downloads/Cloud-Computing-Overview.pdf
148 https://www.bsi.bund.de/EN/Topics/CloudComputing/ESCloudLabel/ESCloudLabel_node.html
149 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2016-02.pdf?__blob=publicationFile&v=4

- **SecNumCloud** - The ANSSI takes a very different approach. The Référentiel SecNumCloud, which is strongly oriented to the ISO/IEC 27001 standard and which supplements it with several specifications of its own, defines the standards required for secure cloud computing. In the Référentiel, there are two levels: sécure and sécure plus, whereby the latter sets higher security standards and limits to France the service provided. Taking this as a basis, the ANSSI has developed a completely new certification of its own, which it has established in France. Cloud providers receive a certificate which is issued by the ANSSI and on which an audit report produced by ANSSI certified auditors is based. For example, providers who want to be certified with SecNumCloud can be audited by AFNOR Certification[150].

While the security levels which the BSI and ANSSI would like to see in place are very similar, **the two very different approaches towards certification and attestation appear to contradict each other**. Moreover, the list of applicable standards and certification schemes for cloud computing across Europe includes, among others: ISO 27001/2, ISO 20000 (ITIL), CSA Open Certification Framework (OCF), Eurocloud, Star Audit, SOC 1-2-3, PCI – DSS, Europrise, FISMA, Cloud Industry Forum Code of Practice, ISACA COBIT, Security Rating (Leet security), TUV certififed.

Motivated by the German-French business consultations[151] and based on a high level of mutual trust, the idea therefore emerged of generating a **new Cloud Label**. It stands for the joint cloud security standards and is suitable evidence that they have been met. The underlying principle on which the label is based is a joint short catalogue with security targets ("core rules"). Naturally, the attestation in accordance with the BSI's C5 and the ANSSI certification are sufficient to meet these standards. **A provider who already has one of the two certifications can receive this label and as such advertise the security level of their product very easily on both markets.** The Cloud Label is regarded by the ANSSI and BSI as being an explicitly European initiative, which can also incorporate the certifications of other countries. In this way, the expertise and independent nature of the BSI and ANSSI, as well as their cooperation based on trust, are of benefit to the whole of Europe.

Another European initiative towards a unique approach for ICT security certification schemes comes from **Horizon 2020 Programme**: the project EU-SEC[152]. The EU-SEC, started at the beginning of 2017, will last until 2019 and aims to create a framework under which existing, certification and assurance approaches can co-exist. Furthermore, it will feature a tailored architecture and provide a set of tools to improve the efficiency and effectiveness of current assurance schemes targeting security, governance, risks management and compliance in the cloud.

Cost Analysis: An economic paper by economists of DG ECFIN estimated that the cost associated to differences in technical rules and multiple testing/certification are between **2% to 10% of companies annual turn-over[153]**. According to this paper inadequate standards and insufficient mutual recognition, including in the ICT sector, is among the main barriers to the single market. For example, the costs of an ISAE 3000 implementation project, in order to be certified under the Cloud Computing Compliance Controls Catalogue (C5) Scheme, can vary from **ten thousand USD up to a million USD or even more**[154]. The costs for enterprises of product conformity assessment can be substantial and there is lack of mutual recognition which implies the multiplication of such costs: for companies offering several product types on a national market of a receiving Member State the costs amount to approximately 2% of their entire annual turnover on that market, whereas they can reach up to 10% for companies specialized in one specific product type because they do not benefit from economies of scale[155]. Even applying the lower bound of 2% only to 60% of the cyber security market to be conservative (i.e. assuming 40% of the market concerns products for which certification is no require) **the costs of lack of mutual recognition reach a figure in the range of 1.2 billion euro**.

---

[150] http://www.afnor.org/en/news/cybersecurity-vigilance-required/

[151] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2016-02.pdf?__blob=publicationFile&v=4

[152] http://cordis.europa.eu/project/rcn/207439_en.html

[153] Ilzkovitz, F. Dierx, A. Kovacs, V. & Sousa (2007) Steps towards a deeper economic integration: the internal market in the 21st century", European Economy, Economic Papers, No. 271. European Commission.

[154] https://www.isae3000.com/controlreports

[155] Ibid. p. 61

Moreover, many organizations are 'locked' into their ICT systems because detailed knowledge about how the system works is available only to the provider, so that when they need to buy new components or licenses only that provider can deliver. **This lack of competition leads to higher prices and some € 1.1 billion per year is lost unnecessarily in the public sector alone[156]**.

As mentioned in the SWD "A Single Market Strategy for Europe - Analysis and Evidence"[157] a large body of economic studies that show the impact that standard have on economic growth and GDP[158]. **For France the impact on growth is estimated at 0.8 %, for United Kingdom at 0.3 % and for Germany at 0.9 % of GDP**. To put this in monetary terms, DIN (the German Institute for Standardization) estimates that in Germany alone, standards generate up to EUR 17 billion a year. A more recent study from the UK 'The Economic Contribution of Standards to the UK Economy' also confirms that the use of standards benefits the national economy: standards contributed to around EUR 11 billion of the EUR 40 billion GDP growth in 2013 (2014 prices) and to around EUR 8.5 billion to UK exports159. The same study shows that standards help to enhance quality, with 70 % of respondents stating that standards had contributed improving the quality of supplier products and services. In the econometric models supporting such estimates standards are considered, together with R&D expenditure and patents, as fuelling the knowledge input in the classical production functions. One key hypothesis is that standards can, to some extent, counterbalance some well-known market failures and the possibility that investments in knowledge by private players are sub-optimal and not sufficient to produce social surplus (externalities).

Benefits for the Cloud Computing Industry of an EU wide Certification Framework: In a world that is increasingly interconnected, it does not make much sense for a State to tackle digital security issues on its own. The new French digital security strategy states France's will to engage a dialogue both within multilateral organizations and with long-term trustworthy partners following two objectives: contributing to the global stability of cyberspace as well as reinforcing the States' own cybersecurity.

The longstanding and close bilateral cooperation between ANSSI and BSI is based on trust and has been greatly facilitated by a shared vision on many strategic and political issues, a common positioning at the national level fulfilling only defensive missions and a comparable high level of technical expertise.

ANSSI and BSI have been working together in many fields, such as cloud-computing with the creation of a common label for secure cloud service providers, security certification though a very strong support of the international recognition schemes (CCRA and SOG-IS) and industrial synergies. An EU wide certification framework could guide these initiatives in order to avoid the fragmentation of standards and certification schemes across Europe and the further development of national approaches. The benefits of standardization through an EU wide certification scheme include, among others:

---

[156] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013DC0455&from=EN

[157] Brussels, 8.10.2015 SWD (2015) 202 final, accompanying the document Upgrading the Single Market: more opportunities for people and business (COM (2015) 550 final) {SWD(2015) 203 final}).

[158] Among peer-reviewed journal articles see: Acemoglu, D., G. Gancia and F. Zilibotti (2012), 'Competing Engines of Growth: Innovation and Standardization,' Journal of Economic Theory, 147, 570–601;Blind, K. and A. Jungmittag (2008), 'The Impact of Patents and Standards on Macroeconomic Growth: A Panel Approach Covering Four Countries and 12 Sectors,' Journal of Productivity Analysis, 29, 51–60; Jungmittag, A., K. Blind and H. Grupp (1999), 'Innovation, Standardisation and the Long-term Production Function,' Zeitschrift für Wirtschafts- und Sozialwissenschaften, 119, 205–222; Wakke, P., Blind, K.; Ramel, F. (2016): The impact of participation within formal standardization on firm performance, Journal of Productivity Analysis 45 (Issue 3), 317–330; Wijen, F.H. (2014). Means versus ends in opaque institutional fields: Trading off compliance and achievement in sustainability standard adoption. Academy of Management Review, 39 (3), 302-323.Swann, P. (2010), International Standards and Trade: A Review of the Empirical Literature. Report for the UK Department of Business, Innovation and Skills (BIS). OECD Trade Policy Working Papers. Among reports commissioned by standardization bodies see: SCC (2007). Economic Value of standardisation; AFNOR (2009). The Economic Impact of standardisation; DIN (2011). The Economic Benefits of standardisation; Standards Australia (2012). The Economic Benefits of standardisation; Cebr (2015). The Economic Contribution of standards to the UK Economy; Cebr (2016). Economic Contribution of Standards in Ireland – A report for the National Standards Authority of Ireland.

[159] British Standards Institution (BSI), 'The Economic Contribution of Standards to the UK Economy', 2015

- **Competitive Advantage**. Companies are motivated to participate in standardization because they gain an edge over non-participating companies in terms of insider knowledge. Early access to information is valuable;
- **Cost Reduction**. Standardization lead to lower transaction costs in the economy as a whole, as well as to savings for individual businesses. transaction costs drop considerably as a result of standards, since they make information available and they are accessible to all interested parties;
- **Supplier/Client Relationship**. Standards can help businesses avoid dependence on a single supplier because the availability of standards opens up the market. The result is a broader choice for businesses and increased competition among suppliers;
- **Standards and R&D**. Businesses not only reduce the economic risk of their R&D activities by participating in standardization, but can also lower their R&D costs. When a company can influence the content of standards to its advantage, the economic risk is lower. The expense of R&D is potentially reduced when the participants in standards work make their results generally available, and research need not be duplicated
- **Raising Trust**. An annual report featured on eWeek[160] shows that 73% of survey respondents are worried about cloud computing security. An EU wide Certification Scheme could raise the trust level of companies in the Cloud Computing services, reducing insecurity due to the various jurisdictions of different Countries.

Conclusion: Even if States are primarily responsible for their national digital security, it is France and Germany's shared vision that many challenges can best be addressed **through a common and coordinated effort at European level.** This could be guaranteed introducing an EU wide certification framework, which avoids multiplication of national approaches, duplication of efforts and waste of resources. Beyond the development of EU Member States' capacities and cooperation, the EU must as well recognize that European digital security is challenged on other fronts, requiring a collective ambition to guarantee Europe's digital sovereignty. Three challenges in particular are ahead of us[161]:

- The EU and the Member States' ability to protect and defend the EU institutions, the administrations, the critical infrastructures, the companies and the general public in cyberspace must be ensured;
- The EU must actively support the development of sustainable European industries in the field of digital security and guarantee Member States' ability to evaluate and approve the security of digital products and services;
- The EU must preserve its capacity to choose autonomously how data and related services should be protected in Europe.

Along with like-minded Member States, France and Germany will closely work together to promote the European digital strategic autonomy, a long-term guarantor of a cyberspace that is more secure and respectful of European values.

[160] http://www.eweek.com/cloud/companies-worry-about-security-implications-of-cloud-services
[161] Federal Office of Information Security, BSI, Security in focus, Europe and International Cooperation, BSI Magazine 2016/02