SPARTA

D11.3

Cybersecurity evaluation facilities

Project number	830892
Project acronym	SPARTA
Project title	Strategic programs for advanced research and technology in Europe
Start date of the project	1st February, 2019
Duration	36 months
Programme	H2020-SU-ICT-2018-2020

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D11.3 / V1.0
Work package contributing to the deliverable	WP11
Due date	July 2021 – M30
Actual submission date	5th August, 2021

Responsible organisation	LEO
Editor	Mirko Malacario
Dissemination level	PU
Revision	V1.0

Abstract	This deliverable will aim to make SPARTA partner cybersecurity evaluation facilities available with support for European and different national cybersecurity certification initiatives
Keywords	Cybersecurity, Evaluation, Certification, Standard, SME, Process, European Cyber Act

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 830892.

Editor

Mirko Malacario (LEO)

Contributors (ordered according to beneficiary numbers)

Assia Tria, Herve Guillaume (CEA)

Andrea Morgagni, Claudio Porretti, (LEO)

Reviewers (ordered according to beneficiary numbers)

Fabio Martinelli, Artsiom Yautsiukhin (CNR)

Bertrand Lathoud (SMILE)

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Executive Summary

This deliverable focuses on Cybersecurity Evaluation Facilities in the context of product and service security certification (e.g. CC and other standards listed in the document).

There is currently a very large plethora of security certification schemes worldwide. This vastness is due to a large number of very different aspects, ranging from simple geographical differences (each nation in the world interprets security issues in its own way) to those strictly related to technical aspects (security has many facets that cover different aspects of the same problem, e.g. Cybersecurity, physical security, privacy, safety, etc.).

Despite all these differences, the actors participating in this context belong to well-defined categories.

A very important category is that covered by the Evaluation Facilities. They have the task of carrying out the most demanding work in a certification process of ICT systems. Indeed, to verify that adopted security countermeasures are operating in the "correct" and "sufficient" way, they go to deeply analyse software codes, among the micro components of a hardware architecture and still in the flow of data exchanged in any communication channel.

The purpose of this document is precisely to show starting from the multiplicity of existing situations what are the structure, skills and tools adopted by the current Evaluation Facilities and how they could change with the evolution of the world to which they belong.

The document describes also how could be possible to improve the cost-effectiveness of the cybersecurity certification in particular taking into account two main themes:

- In developing critical products that have to be certified the developer should adopt an approach “Security as a process” in order to address since early stages of the product development the future cybersecurity certification.
- Evaluation Facilities and Certification Body of the different schemes could improve the cost-effectiveness of cybersecurity certifications by improving and formalizing a collaboration network for making re-use of evidences, tools and experiences gained in the different field of cybersecurity certifications.

Much of the terminology adopted within this document derives from the Common Criteria international standard (ISO 15408, Ref. [4]), which provide a unified and comprehensive framework for security evaluation and inspire many certification schemes. However, it is important to emphasize that the intention is not to impose this standard as a unique solution for a possible unification of the schemes.

Table of Content

List of Figures

List of Tables

Chapter 1 Introduction

Each part of our everyday life is closely linked to the sector of "Information and Communication Technologies (ICT)". Just thinking banally about the news we receive daily from the media, the more or less sensitive information that we exchange on electronic devices (mobile phones, computers, etc.) both in our private life and in our work activities.

Even actions that - seem to be light years away from these concepts are closely related to this sector.

Two striking examples of this statement are the following: filling a glass with fresh water that comes out of the tap at home (e.g. through Smart Water Grid system able to supply water) or turn on the light in a room when darkness falls (e.g. through Smart Grid Distribution and Smart Meters). Smart Grids are constituted by Operational Technologies (OT) and Information and Communication Technologies (ICT). The digitalisation reduces the distance between "OT and ICT with the clear objective of improving our lives.

None of these seemingly unrelated actions could take place nowadays without an effective and operational ICT infrastructure. However, we have to consider also the downside.

The technologies globalization leads us to new - risks affecting different sectors.

In particular, our attention is focused on problems related to Cybersecurity that nowadays affects all those aspects that are essential for the life of our society and that can lead to Cyberterrorism attacks.

Two famous examples of modern impacts of Cyberterrorism have been the following:

- The first is Stuxnet, one of the most destructive computer viruses ever made. Stuxnet spreading mainly via USB sticks. Its target was controllers from one specific manufacturer. The first target of the virus was the Iranian Natanz uranium enrichment plant. (Ref. [12])) but the malicious code, due to uncontrolled use of USB sticks, arrived on the internet having a worldwide diffusion.
- The second was Ukraine power grid cyberattack. It took place on December 2015 and is considered to be the first known successful cyberattack on a power grid. Attackers were able to successfully compromise information systems of three power distribution companies in Ukraine (Ref. [13]) and temporarily disrupt electricity supply to the end consumers for several hours (Ref. [14]).

Cybercrime is now a daily concern for public and private bodies, companies and individual citizens. Cybersecurity statistics indicate a significant increase in data breaches and hacking, most of which concern devices in the workplace.

The following lists, summarized from a set of studies carried out recently, highlights just some numbers related to cybersecurity attacks worldwide.

- Data breaches exposed 4.1 billion records in the first half of 2019. (source RiskBased [14])
- Tactics used by attackers: 45% of breaches featured hacking, 17% involved malware and 22% included social attacks (e.g. phishing or social engineering, respectively). (source Verizon [15])
- 86% of breaches were financially motivated. (source Verizon [15])
- Average number of security breaches are increased by 11% from 2017 to 2018 and increased by 67% in the timeframe 2013-2018. (source Ponemon Institute sponsored by Accenture [16])
- The average time to identify a breach in 2019 was 206 days (about 7 months) and the average lifecycle of a breach (from the event of the breach to its containment) was 279 days, (about 9 months). (source Ponemon Institute sponsored by IBM Security [17])

So it’s clear how the Information Security (in terms of confidentiality, availability and integrity of our data) is important for us, for our business or organization and we have to create an information security culture in order to spread how important it is to protect data that means protecting ourselves and our society.

Furthermore, because prevention is better than cure, in order to prevent cyber threats, it is important to define a strategy to protect data, infrastructures and the people.

From a user point of view knowing that a critical product has been certified allows to reduce the feeling of the constant danger to which we are subject in the world of technology.

Certification defines rules which once respected through verification processes, allows to reduce the overall attack surface and can increase the trust that we place on products systems and processes adopted in the ICT sector.

The SPARTA project moves precisely in this direction. In particular, the WP11 goal is to ensure that project roadmap and Programs are aligned with international, European and national certification program for SW and Products.

Well-defined Cybersecurity Certifications permit to implement comprehensive, valuable, and repeatable processes, saving time without reinventing the wheel each time new technology is invented and implemented or new threats appear, or regulations are released.

This perspective attracts the attention of several nations worldwide and new initiatives have been started in recent years to establish high-level cybersecurity requirements for ICT components on traditional infrastructures, including requirements for certification processes. The definition of an ICT security certification framework allows, for example, the ICT vendors to perform a single certification process instead of several certification process depending the target state where the products will be sold.

In order to avoid risks such as market fragmentation and challenges to interoperability, these initiatives need to be integrated with each other.

This approach, in EU Member States, is well delineated by recent legislative and political developments such as:

- the adoption of the NIS directive[1]
- the Cybersecurity Act[2].

In this process ENISA, the European Network and Information Systems Agency, acts for supporting the EC and Member States in developing a certification framework for ICT security products and services, aiming to promote the mutual recognition of certificates and the harmonization of certification practices. When we talk about certification, we need to talk also about a third-party evaluator that performs evaluation activities in a certification. This third party is represented by laboratories that in the following we refer as “Evaluation facilities”. For these reasons their contributions become fundamental.

Laboratories can belong to government agencies, to military, to private companies and so on. In any case they must make their fundamental contribution in the certification processes by focusing on their expertise and independence

The purpose of this document is to identify and analyse, considering the existing schemes and the standards in use, the panorama of the current evaluation facilities through their organization, their knowledge base, their tools and to propose the direction of their possible evolution in this changing world. This can help also to define how the cybersecurity facilities could evolve to support the latest versions of cybersecurity certification scheme.

Furthermore, another example of evolution is narrowing the distances between research and certification. This could be reached, for example, by using competences of Research Institute Subject Matter Experts (SME) in cybersecurity certification process or by using complementary

[1] a directive introduced to better protect the network and information systems of operators of essential services and of digital service providers, to ensure the general functioning of the crucial services for citizens and businesses (https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive)

[2] an EU-wide cybersecurity certification framework for digital products, services and processes (https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act)

software tools, developed in R&D programs, for performing security activities during cybersecurity certification.

On the other hand, this document addresses the issue of improving the cost-effectiveness of a cybersecurity certification from the developer of critical products point of view.

In developing critical products that must be certified, the developer should adopt an approach “Security as a process” in order to address since early stages of the product development the future cybersecurity certification.

Chapter 2 Certification in Cybersecurity world

2.1 A generic concept of certification

If in any dictionary, we do the research of term “certification” we would find something like this:

The action or process of providing someone or something with an official document attesting to a status or level of achievement (Oxford dictionary).

In particular, the certifications, performed in in accordance with specific standards and other applicable technical documents, can be grouped in:

- Systems Certifications: they ensure that the system implemented by a generic organization, public or private, of any sector, complies with current standards. In this context, the system can cover the most varied issues, from quality management, environmental issues and the sustainability of events, health and safety in the workplace, information security and IT services, energy, security in the supply chain, business continuity, etc.
- Certifications of products and services: they can concern an asset, a service or a process. The evaluation for the purposes of certification naturally concerns only some characteristics of the object under certification. In particular, those contained in the reference standard or technical specification. Through the certificate, the manufacturer or supplier can demonstrate to the market his ability to obtain and maintain compliance with a set of obligations of the products manufactured or the services provided.
- Certifications of people: they certify the possession and maintenance over time of the skills and competences that make professionals suitable for carrying out certain activities. The certificate of conformity represents the formal recognition, by a third-party body, also in this case independent from the assessed person, of the necessary requirements to be able to operate competently in a specific sector of activity. The certifications motivate the professionals to acquire, maintain and continuously improve the necessary skills over time.

The second category, that is the one relevant to the SPARTA Project, is analysed in the following sections.

2.2 Introduction to Cyber security evaluations/certifications (Advantages and Limits)

After this brief introduction on the general concept of certification, we focus our attention to the main objective of the project, certification in the context of “Cybersecurity”. With this intention we analyse how the concept of security has evolved in the last decades to face what have been the related problems that have arisen with the passage of time and with technological developments.

Evaluation and certification have a long history and they accompanied the technological process by giving each other ideas for evolution.

Since 1800, the intensification of number of boiler explosions, due to the increase in pressure adopted within them, led insurers to devise the definition of a certification procedure. On the other hand, these growing risks have also led innovation toward “non-explosive idea” of water tube boiler.

In 1892, William Merrill under the impression of the commercialization of electricity founded the Underwriters Laboratories (UL). This is because, due to the increasing number of fires produced and the scarce existing countermeasures, he began to evaluate products such as fire doors and fire extinguishers on behalf of the insurance sector within his laboratories.

UL currently boasts over 1,000 security standards and over 20,000 evaluated products.

Evaluation and certification development have proved more difficult in the world of information security, where they have had a reasonably long history in which it is possible to highlight the advantages and limits of its development.

In the early 1970s, USA government users recognised that the security offered by commercial computer systems was poor. It seemed to be no way for improvement; as soon as one vulnerability was resolved, another one was immediately exploited.

This led the US government to commission a study [1] which introduced an important recommendation: the security of operating systems should be reduced to that of a protection component that made it small and simple enough to be subject to analysis and testing, such as to guarantee its completeness (advantage).

This subsequently led to the promulgation of a security standard, Trusted Cyber Security Assessment Criteria, also known as the "Orange Book" [2].

The Orange book provided the criteria for classifying the Security System into a series of levels - C1, C2, B1, B2, B3 and A1 - depending on how carefully the mechanisms were designed to ensure the confidentiality of classified information.

The Orange Book certification produced a first market for the evaluated systems.

However, evaluation meant subjecting a system to careful consideration by engineers from the National Computer Security Center, a division of the NSA.

In this process, however, a vendor needed a government sponsor to get a candidate system to support this process, and once inside, it often took 2-3 years.

Therefore, the costs were as high as the timing. The result was that certified products was not with state-of-the-art technology (limit).

Europe answer to the Orange Book was not long in coming. In 1990 was published the first version of "Information Technology Security Evaluation Criteria" (ITSEC) [3].

In this model, the first big change was that the evaluation process was performed by commercial laboratories paid by a vendor and regulated by the government. The introduction of new actors in the certification process increased the interest of private companies in these practices and contributed to provide greater assurance to final users in view of that a third-party assessment confirmed the security claims of a vendor (advantage).

This was the first advent of laboratories as third party “actors” in IT security certification process.

Most likely, this solution was successful, and the results achieved shortly thereafter.

After the end of the Cold War, the European model prevailed creating the Common Criteria for Information Technology Security Evaluation (ratified as an international standard in 1999) [4].

Common Criteria use commercial laboratories, called "Commercial Licensed Evaluation Facilities” (CLEF) to keep it that way but has also introduced further innovation.

The attention of the authorities in the creation of this structure was that of expanding the certification processes to a much wider range of applications, in the hope that this enhancement improves the number of products evaluated and lowers costs.

While the Orange book was focused on the protection of classified information, the Common Criteria introduced the concept of evaluation against a model called "Protection Profile" (PP). Through the Protection Profile it is possible to define a profile of potential threats and protection that can be put in place in order to counter those threats (advantage).

This approach aroused the interest of a greater number of actors who actually saw, in the definition of a Protection Profile (PP) dedicated to a certain category of products, security features, the way to have items from the market that, following those directives, could satisfy their desires and increase the security of the products / systems / processes adopted by them. PPs, in fact, allow to “standardizing” and “comparing”, easily, from a security point of view, a set of products belonging the same class (Network Devices, Operating Systems, etc.) helping vendor and customers in guiding their choice (advantages).

In fact, over time, the interest in protection profiles has not only stimulated the imagination of governments and large companies in specifying their requirements, as part of their acquisition process in search of "lost or never acquired security". PPs have also favoured the proliferation of groupings of users in communities, in order to express their desire for security and of developers of particular categories of objects in defining the basic security requirements that their objects could satisfy.

In this way, Common Criteria have had the opportunity to be used for evaluations in a large number of new areas of application, starting with smart cards and moving forward with new technologies such as current products in the world of IOT.

Thanks to its flexibility (advantage) highlighted in the previous statements, this approach has found fertile ground also in this project.

Demonstration is set in Task 5.2 of WP5 in which ad hoc PP for the vertical 1 has been defined and in which we have gone even further by inserting in such a format alongside the security requirements those of safety [9].

Of course, these evaluation and certification processes also have a downside and they have to focus on these aspects to improve themselves in the future.

- These processes, most of the time, adopt defined and sometimes complex languages to understand (limit); it must be considered even if this is should be a non-recurrent cost (learning phase, frequently with the support of consultants or evaluation labs).
- Security must be seen as a process and therefore it must be addressed in an appropriate way in all its phases. Poor management of some of its phases may lead to failures that may discredit the evaluation / certification processes, even if their soundness is not in cause.
  To better understand this statement and better use the concept of security as a process, we can introduce some lessons learnt starting from analysing mistakes of the past / present related to the understanding of the certification process and hypotheses.
  Starting from the considerations made on the PPs, a first example that has validity in general is that any PP must be taken for what it is, and considering the assumptions on which it is based. It is necessary to understand that conformance to a PP will never solve all the security problems of a certain object but only those addressed by the PP on the basis of well-defined hypotheses on its operating environment.
  The same type of reasoning can be done on different types of certifications.
  In the example we consider the evaluation of a cryptographic hardware according to the FIPS-140 standard in which a high-level certification (4) indicates that the device is tamper-proof, which means: “there is no possibility of carry out a physical attack to the object successfully in order to extract the keys protected by it”. But in the case of the IBM 4758 device certified at level 4 according to the FIPS standard, it was possible. However, this information was obtained through a software attack and not attacking the certified Hardware [5].
- Another element that tends to discredit a certification is that it refers to a product or system in a certain configuration and at a certain date (limit).
  There are plenty of examples to consider in the past.
  Many of certified Microsoft's operating systems have suffered attacks related to an identified vulnerability after obtaining the security certification. This has happened because certifications of these products are limited to a certain configuration in a certain date (including security patches). "Static" certification is in contrast with the current situation, which includes rapidly evolving attackers and new vulnerabilities.
  There were also conditions in which the certificate did not coincide with the operational needs of the users. As in the case of Windows NT whose certification was referred to a diskless workstation that allows only a use as a thin client, not considering the classic configurations in the real world. Nowadays, the growing usage of agile development methods, and in particular the success of the DevOps approach, is very challenging for a certification approach perceived as static.

> This does not mean that if, along life cycle of a product/system, the surrounding situations change, the certification is no longer valid.
> New vulnerabilities could be introduced both by a change in the operating environment or configuration, but also by the development of new technologies. But this statement cannot be translated into the assertion “the evaluation / certification process is useless”, considering that the same process has eliminated, with a certain level of assurance (evaluation / certification level), all security issues in a certain operating environment, for a well-defined configuration and in a precise moment of its life cycle.

Then the certification, as well as being a significant cost for the vendors, proved to be counterproductive by discrediting the value of the product to end-user’s eyes, instead of bringing the advantages hypothesized by a similar process.

However, we have to underline that in all circumstances the security of the object was not considered throughout its life cycle.

In the next table there’s a summary of advantages and limits of these kind of processes evidenced in this paragraph, by a general point of view (developer involvement, benefits for the target, lack of the process, etc.).

Limits	Advantages
• Process is complex to manage (evaluation, certification, acceptance) • Cost for the evaluations • Long duration hampers time to market • No shared risk analysis between actors • Shallow learning curve • Complex language needs learning phase	• Process is performed for one product to address one or several customers. • Certification enforces standardization • Established terminology and definition of requirements with work packages and tasks. Labelling and definition of security/assurance level • Objectivity and independence of evaluation labs • “impartiality and repeatability of security certification • Multiple developers benefit from the expertise of evaluation labs, ensured by specialization, experience and authorization by the owners of the certification schemes, • Effectiveness of the process • Certification requirements are used by risk owners in their RFPs and ensure a level playing field for suppliers • Evolution of process covers changing environmental and technical factors • Re-usability appropriateness including previous evaluation results • Business opportunity for developers (opening to particular markets, reduce competitors)

Table 1: Evaluations/Certifications Advantages and Limits summary

2.3 Security as a process

Security should be viewed as a process, which should not be static. Moreover, it must be easily modifiable so that any improvement can be implemented, and it must cover the entire life cycle of the target (product, system or process) to which security is applied.

As we observed at the end of the previous paragraph, one of the problems that arise with a static type certification is that the validity of the certifications would seem to decay when the first patchless vulnerability is highlighted.

This leads on one hand to push towards the patching of vulnerabilities, but on the other hand it is necessary that such patching, if relative to a certified target, needs the definition of an appropriate procedure that goes to consider the correct actors (those of the certification process) and accompanies this target throughout its life cycle.

But this is only one aspect of one of the phases of what we can introduce with the name of "Security Process".

Let's then consider what the approach to safety, adopted in the CAPE program of this project, was and in particular in deliverable D5.1 [8].

In this context, security in general has been approached as an iterated process, and it has been shown that the identified process is applicable to different frameworks of interest.

In particular, the same process has been adapted to the following contexts:

- Common Criteria Evaluation Process
- Safety engineering
- Security engineering

using the V-model as shown in the following Figure 1 (acronyms described in Chapter 8).

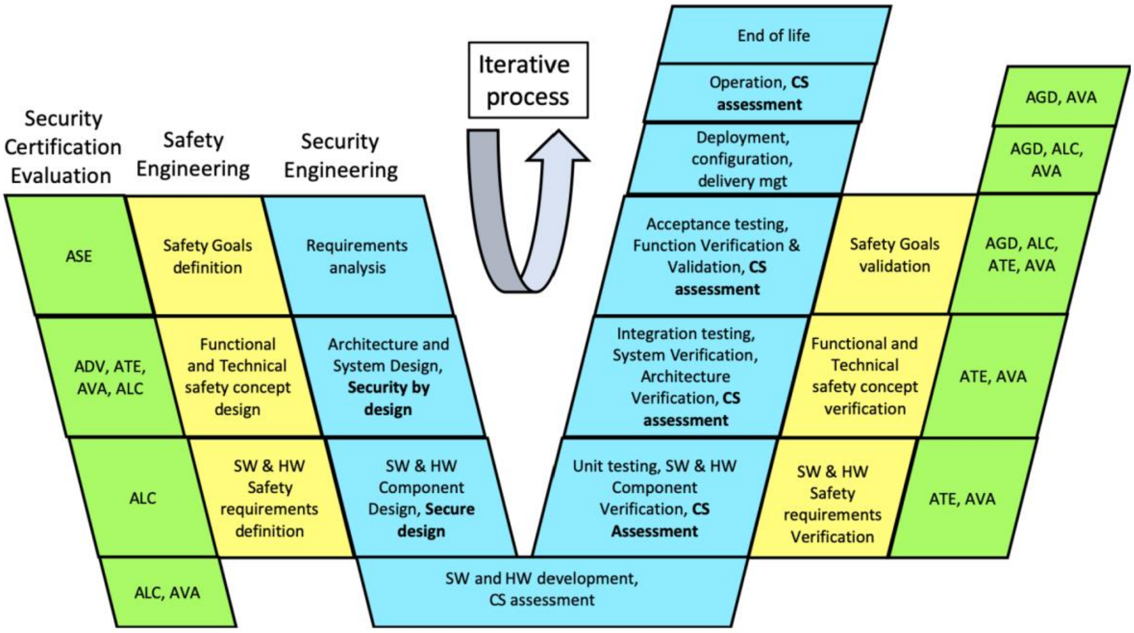

Security Certification Evaluation
Safety Engineering
Security Engineering
Iterative process
ASE
Safety Goals definition
Requirements analysis
ADV, ATE, AVA, ALC
Functional and Technical safety concept design
Architecture and System Design, Security by design
ALC
SW & HW Safety requirements definition
SW & HW Component Design, Secure design
ALC, AVA
SW and HW development, CS assessment
Unit testing, SW & HW Component Verification, CS Assessment
SW & HW Safety requirements Verification
ATE, AVA
Integration testing, System Verification, Architecture Verification, CS assessment
Functional and Technical safety concept verification
ATE, AVA
Acceptance testing, Function Verification & Validation, CS assessment
Safety Goals validation
AGD, ALC, ATE, AVA
Deployment, configuration, delivery mgt
AGD, ALC, AVA
Operation, CS assessment
AGD, AVA
End of life

Figure 1: Different frameworks V-model appliance

All of these, however, can be traced back to a flow process relating to the security assessment that can be generally applicable to a product, a system (of any complexity) or a process, during its entire life cycle, which we can summarize in the following figure.

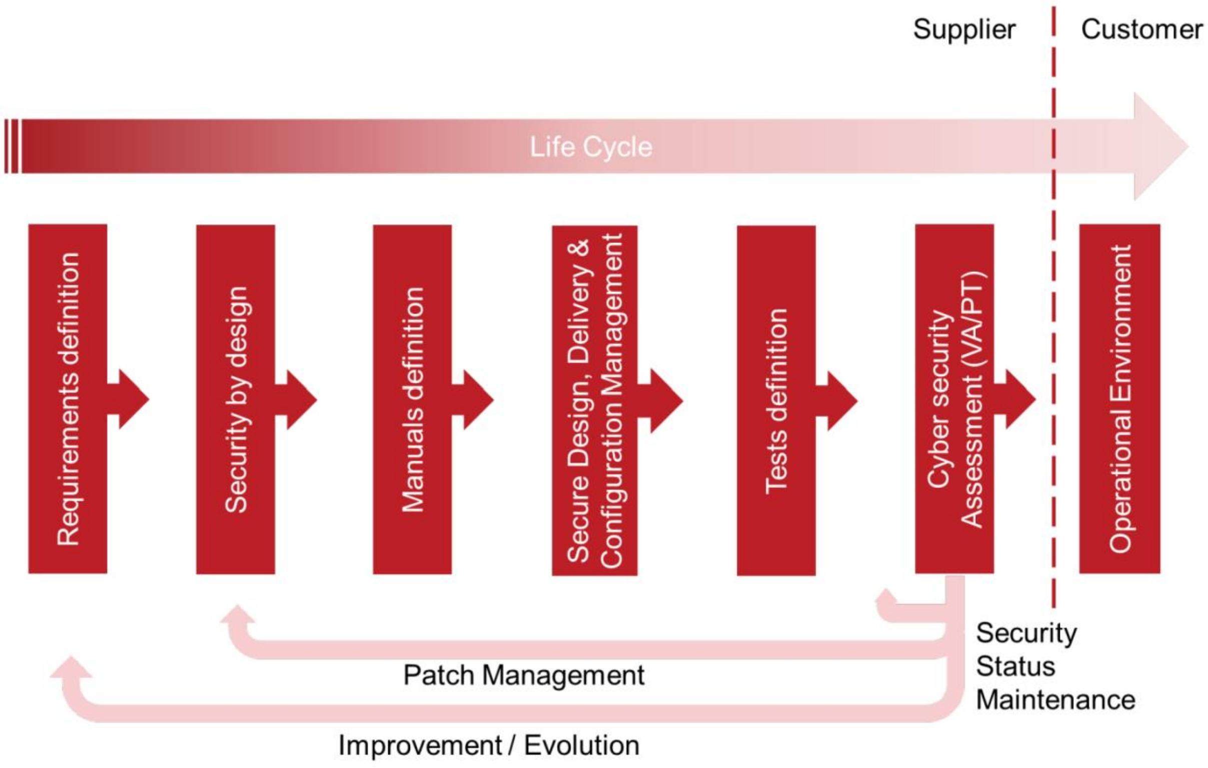


Figure 2: Cybersecurity Evaluability process phases

For demonstration purposes, we can propose the overlap of the phases described in it with those declared in a generic certification process according to standard Common Criteria (ISO 15408 Ref. [4]).

The following Figure 3 represents in a different way what has been introduced with Figure 1 and Figure 2.

In particular Figure 3 has the objective to highlight the following: if a "security by design process" is performed by the developer during the implementation of a new system/product, it will be simpler to address the requirements, and to provide required evidences, of a standard such as Common Criteria.

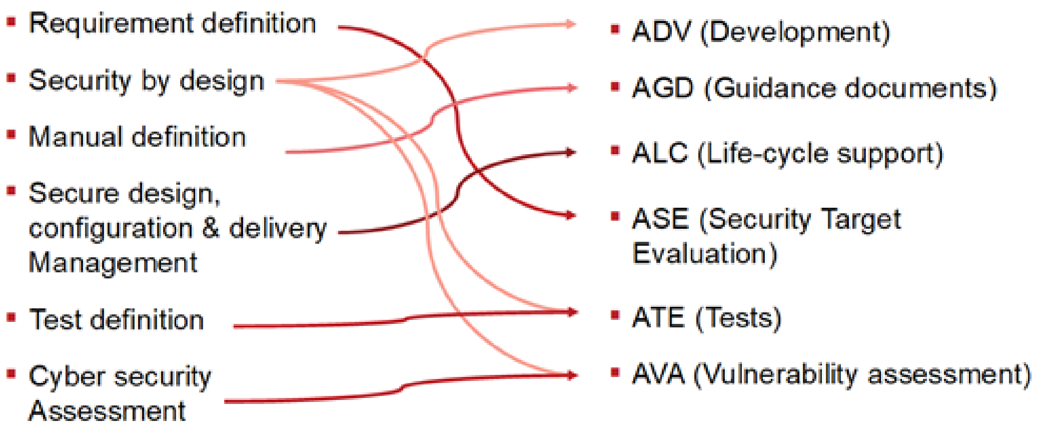


Figure 3: Common Criteria Assurance Classes mapping

In fact, if the development process is carried out having in mind the subsequent cybersecurity certification of the product/system, the cost of:

- providing certification evidences
- performing the certification itself
- managing updates

will be lower. The development process must consider security aspects in the whole life cycle.

However, it is important that the process is not focused only to the development phase. The process has to consider also the patch management/improvement activities (see also limits in section 2.2) in order to provide more efficiently the evidences for maintaining the certificate obtained for the evaluated product (this is the importance of the three feedback arrows in Figure 2: Security Status Maintenance, Patch Management, Improvement / Evolution).

This aspect, in particular, is under investigation within the task 5.4 of the CAPE program by analysing how make faster the incremental certification/assurance continuity and the development of Impact Analysis Report by using DevSecOPs.

Even if the "security" has become fundamental in the last year, at the moment a lot of product/systems are developed in a "functionality-driven" way by considering security as an add-on. This approach, typically, implies that need of extra-effort for performing cybersecurity certification and its maintenance.

For this reason, becomes fundamental to stress the concept of "Security as a process".

What is shown in the previous figure can be summarized with the description of the correlation between the assurance classes and the Cybersecurity process phases, as follows:

In the following, we report the description of Common Criteria assurance classes as described in deliverable D5.1 of the CAPE SPARTA program [8]:

- *"ASE (Security Target Evaluation): this class deals with the evaluation of the consistency of the "Security Target" (the scope of the evaluation) which also contains the definition of the security requirements of the Target Of Evaluation (TOE, the subject of the evaluation), therefore it is closely linked to the security requirements management phase".*
- *"ADV (Development): this class deals with the evaluation of the six families of requirement for structuring and representing the security functionality realized by the target of evaluation (TOE) at various levels and varying forms of abstraction that the developer must produce during the product development phase, naturally it is linked to the features of the Secure by design processes adopted by the supplier".*

- *"AGD (Guidance Documentation): this class takes care of the evaluation of the manuals that are delivered to the customer. These manuals contain both the secure configuration process of the TOE in its user environment and its safe use methods for each category of defined end-user".*
- "ALC (Life-cycle support): this is a very important class that evaluates all aspects of the *management of the TOE during its life cycle: in the development phase in which it is under the responsibility of the developer, during the transitional phase of transport in its final operating environment and of course the management in the operating environment under the responsibility of the customer and the developer, in the hypothesis of maintaining the certification (security patch management)".*
- *"ATE (Tests): it is the class that takes into consideration all the tests that demonstrate that security functionalities operate according to its design descriptions, both the functional ones proposed by the developer and the independent ones proposed by the evaluators".*
- *"AVA (Vulnerability Assessment): this class takes care of vulnerability assessment activity to analyse vulnerabilities in the development and operation of the TOE. Development vulnerabilities are those introduced during its development and these can be minimized with the adoption by the developer of" security by design" processes. Operational vulnerabilities are those that could exploit the weaknesses of non-technical countermeasures to violate the TOE security functionality. This analysis is carried out by the evaluators during TOE evaluation deliverables analysis or from the classic vulnerability analysis performed also adopting automatic tools".*

Of course, in such a process, compared to a normal CC certification process, to maintain the status of the target obtained with the certification, some of these phases must be repeated throughout its life cycle. This is represented in figure 2, by means of the feedback forms indicated with the expression "Security Status Maintenance" which includes "patch management" and "improvement / evolution" processes.

The possibility of applying this process to different frameworks and to different targets becomes an interesting challenge for the future, also considering the situation that is currently emerging in Europe.

These considerations increase the importance of addressing, in the certification schema, the needs, and challenge, of establishing cost-effectiveness requirements for Security Status Maintenance (or Assurance Continuity). This methodology is fundamental in order to maintain/update the certification of a product/system during its natural evolution.

Chapter 3 The situation in the European context

Europe is aware of these challenges and is developing several answers to tackle them.

The processes launched in the recent past and which are making the greatest contributions at European level to the Cyber-Security theme are the following:

- NIS directive
- Cyber ACT

Let us now try to summarize what the objectives of these two movements are.

3.1 NIS directive

The NIS directive is, without any doubt, the first piece of a legislation at European level aimed at Cybersecurity, in particular to provide legislative measures to increase the general level of cybersecurity in our continent.

The Directive on security of network and information systems (the NIS Directive) was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016, with the aim that member states could subsequently transform this directive into laws to be applied at national level and for the purpose of identifying the operators of essential services on the same level.

In this direction, the NIS directive proposes, for the various member states, to equip themselves appropriately starting from the formation of a cyber-security incident response team (CSIRT) and definition of a competent national authority of the NIS, which is capable of to cooperate with all other states in order to support and facilitate common strategies and the exchange of useful information.

Moreover, there is the purpose to set a CSIRT Network, in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing a full list of information about security across sectors which are fundamental for our economy and society such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

The prerogatives are to define a minimum level of skills standards, or simply roles, within companies. It is not uncommon that the companies, we believe to be most exposed, deal with different approaches and sometimes superficially with significant risks for the system that makes up the nation.

In the second analysis, it is necessary to route communications on a collaborative line.

Once operational, the national CSIRTs must be able to perform various tasks in the cyber security field that can actually contribute to increasing the European security level:

- the definition of procedures for the prevention and management of IT incidents.
- the receipt of incident notifications and activation of alert procedures.
- the supply, to the person who made the notification, of information that can facilitate the effective management of the event.
- the information of other EU Member States possibly involved in the incident, protecting the security and commercial interests of the OSE or the FSD as well as the confidentiality of the information provided.

Lastly, the encouraging aspect from a collaborative point of view is the fact that the CSIRT will have to identify forms of collaboration, through the identification of forms of operational cooperation, the exchange of information and the sharing of best practices.

In this context ENISA should assist the Member States and the Commission by providing expertise and advice and by facilitating the exchange of best practice.

To fulfil its tasks and exploiting its competences The European Network and Information Security Agency (ENISA) has published the framework "Information Security Audit and Self - Assessment

Frameworks for operators of essential services and digital service providers" for the National Competent Authorities (NCA), the Digital Service Providers (DSP) and the Operators of Essential Services (OES).

The study output is a set of good practices for audits and/or self-assessments that meet the security requirements of the directive. In fact, the framework proposes steps to facilitate these processes, building lists of questions to facilitate compliance activities. ENISA considers this report an integral part of its work for a collaboration between Member States in the field of Cybersecurity.

Finally, in order to clarify the legislative status of the NIS directive, ENISA has made public the "NIS Directive tool", an interactive tool that shows the relevant national laws and regulations and, for each sector, the national authorities subject to the directive.

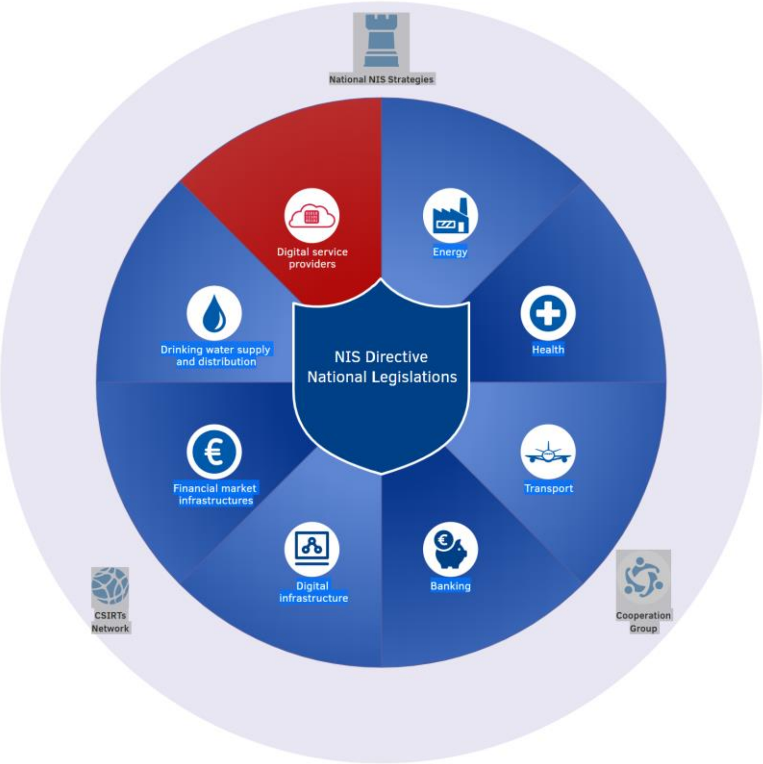


Figure 4: NIS Directive tool interface

3.2 Cyber Security Act

After the approval of the NIS Directive, the European institutions continued to work on measures aimed at strengthening cyber security in the European Union. The main of these measures adopted consists of a Regulation aimed at creating a European framework for the certification of IT security of ICT products and digital services, and at strengthening the role of the European Network and Information Security Agency (ENISA): the so-called Cybersecurity Act.

3.2.1 Cyber Security Act description

This Act constitutes a key part of the new EU cyber security strategy, which aims to strengthen the Union's resilience to cyber-attacks, to create a single cyber security market in terms of products, services and processes and to increase consumer confidence in digital technologies. The regulatory instrument in question merges, and is in part complementary to NIS Directive, that we introduced earlier.

The Cybersecurity Act is structured in two main parts: the first specifies the role and mandate of ENISA, while the second introduces a European system for the certification of IT security of Internet-connected devices and other digital products and services. As this is a regulation, once it enters into force, the Cybersecurity Act will be immediately applicable in all Member States, without there being any need for implementation actions by national legislators, except as regards some limited provisions, for example regarding sanctions.

3.2.2 Importance of the role of ENISA

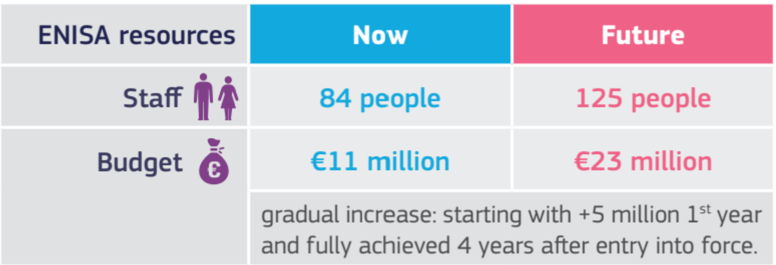
A first key point of the Cybersecurity Act concerns the strengthening of the role of ENISA. The Agency was established in 2004 - with a temporally limited mandate - to contribute to the general objective of ensuring a high level of security of networks and information systems within the EU.

Up to the Cybersecurity Act, ENISA's role has been mainly to assist Member States and European institutions in technical terms in the development of policies on the security of networks and information systems and to strengthen their capacity to prevent, detect and react to cyber incidents. However, the operational management of cyber incidents remains an exclusive competence of the Member States.

The Cybersecurity Act certainly reinforces the role of ENISA through a permanent mandate in which it will no longer perform only technical consultancy tasks but also support activities for the operational management of cyber incidents by the Member States. In this way, ENISA will be able to provide more concrete support, also with respect to the implementation of the NIS Directive.

ENISA will also have a fundamental role in the management of the certification system introduced by the Cybersecurity Act.

This also includes important data for ENISA which indicate a passage of its resources from 84 to 125, with a budget going from € 11 to € 23 million, as indicated in the table.



ENISA resources	Now	Future
Staff	84 people	125 people
Budget	€11 million	€23 million
	gradual increase: starting with +5 million 1st year and fully achieved 4 years after entry into force.	

Table 2: Numbers for ENISA

3.2.3 IT security certification of digital products and services

Another key point of the Cybersecurity Act concerns the introduction of a European IT security certification system for digital products and services. This is also in order to facilitate the exchange of the same within the European Union and to increase consumer confidence in them.

The establishment of specific certification schemes for security of ICT products and systems is not in itself a novelty.

For example, two important international arrangements already ensure cross-recognition of Common Criteria certificates:

- The first one is the Common Criteria Recognition Arrangement (CCRA). It is the base of the Common Criteria. This is the arrangement that allow "*IT products and protection profiles* *which earn a Common Criteria certificate can be procured or used without the need for further evaluation*". (source:. https://www.commoncriteriaportal.org/ccra/index.cfm)

- The second one is the SOG-IS (Senior Official Group – Information System Security) agreement.
  This agreement is of special importance in the European context, all the more so as it ensures cross recognition of certificates up to the highest Evaluation Assurance Levels (EAL 7) in two "technical domains" highly relevant for security: smartcards and similar devices on one hand, hardware devices and security boxes on the other hand.

Besides many other schemes already exist in most Member States. They aim at providing a certification less cumbersome than Common Criteria, at the expense of a lesser level of thoroughness, and a level of assurance usually commensurate with the lesser CC Evaluation Assurance Levels.

For example, in Italy, the "Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione" (ISCOM, operating at the "Minister dello Sviluppo Economico) already certifies the IT security of ICT products and systems according to the national scheme for the evaluation and certification of the security in the information technology sector established by the DPCM dated October 30, 2003. Similar certification schemes also exist in other Member States.

Other examples are the Certification de Sécurité de Premier Niveau des Produits des Technologies de l'Information (CSPN), in France; Commercial Product Assurance (CPA), in the United Kingdom; and the Baseline Security Product Assessment (BSPA), in the Netherlands.

However, these certification schemes are not recognized abroad, or at least not in all Member States.

This forces companies which for any reason are reluctant to Common Criteria evaluation to carry out various certification processes to operate transnationally. For example, the European Commission has verified that a manufacturer of smart meters that intends to sell its products in Germany, France and the United Kingdom must have them certified according to three different schemes. Note that, at the moment, certification costs tend to be quite high for businesses, in a variable between 100,000 euros and one million euros, depending on a large number of parameters.

3.2.4 "European framework" for certifications valid throughout the EU

The Cybersecurity Act aims to remedy the above problems by introducing an overall framework of rules governing European IT security certification schemes. However, it should be noted that the Cybersecurity Act does not establish directly operational certification schemes, but rather creates a "framework" for the establishment of European schemes for the certification of digital products, services and processes. The creation of these certification schemes, to be prepared for specific categories of products, services and processes, will entail that the certificates issued according to these schemes will be valid and recognized in all Member States.

The European certification schemes envisaged by the Cybersecurity Act will be prepared, first of all, by ENISA and then formally adopted by the European Commission through implementing acts. Medical devices, industrial control systems and automated vehicles (topic of Vertical 1 in WP5 of this project) are just some examples of the products for which a European certification scheme is likely to be made available.

Once a European certification scheme has been adopted by the Commission, interested companies will be able to apply for certification of their products, services and processes to specific accredited bodies, unless the certification scheme in question allows companies to carry out a self-assessment of conformity (only for low risk products, services and processes). The use of the certification will however remain voluntary, unless the certification is expressly requested for specific categories of products, services and processes by specific industry standards.

The European certification schemes will gradually replace the homologous national certification schemes, but the certificates issued on the basis of the latter will remain valid until their expiration date.

The following scheme summarize the process (with references to actors[3] and actions) adopted to obtain the definition of a European Cybersecurity Certification Scheme

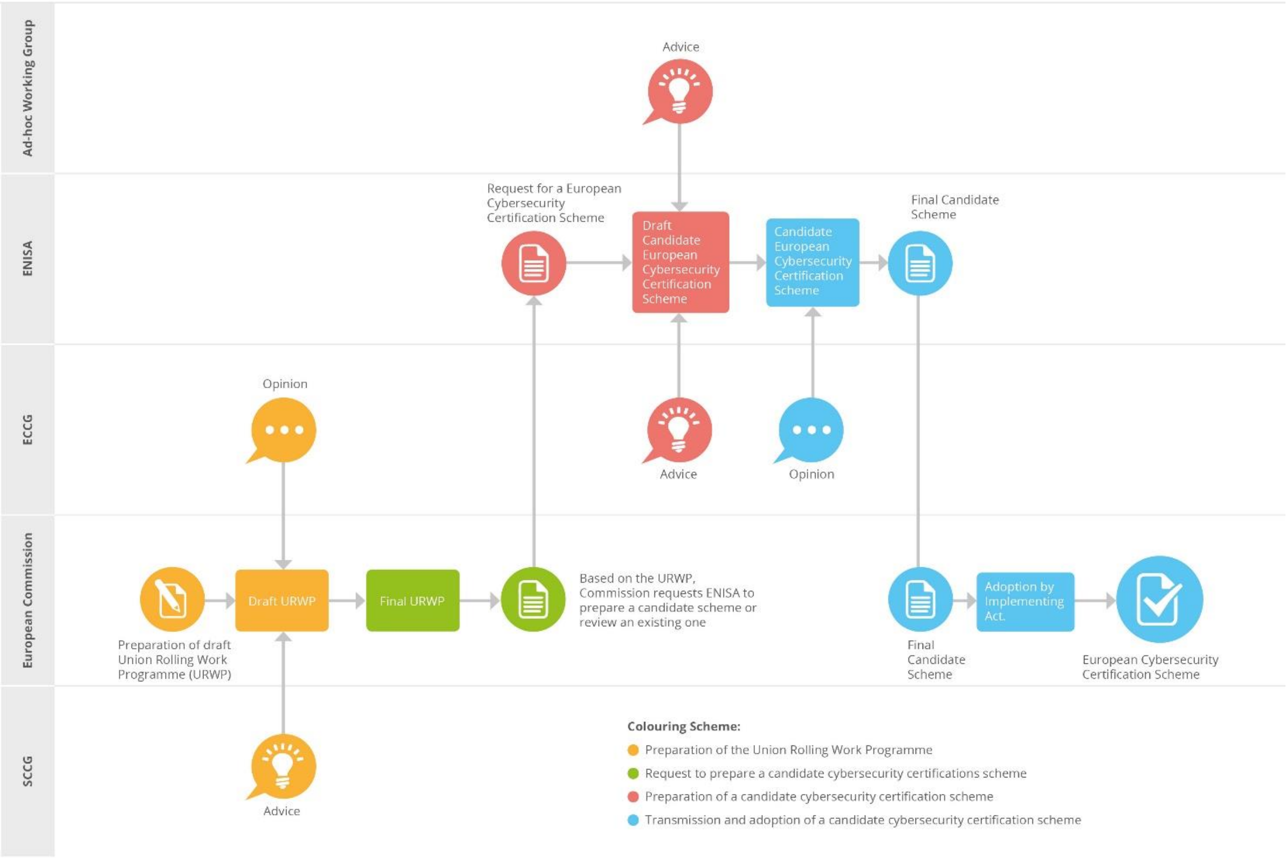

Ad-hoc Working Group
ENISA
ECCG
European Commission
SCCG
Advice
Request for a European Cybersecurity Certification Scheme
Draft Candidate European Cybersecurity Certification Scheme
Candidate European Cybersecurity Certification Scheme
Final Candidate Scheme
Opinion
Advice
Opinion
Preparation of draft Union Rolling Work Programme (URWP)
Draft URWP
Final URWP
Based on the URWP, Commission requests ENISA to prepare a candidate scheme or review an existing one
Final Candidate Scheme
Adoption by Implementing Act
European Cybersecurity Certification Scheme
Advice
Colouring Scheme:
● Preparation of the Union Rolling Work Programme
● Request to prepare a candidate cybersecurity certifications scheme
● Preparation of a candidate cybersecurity certification scheme
● Transmission and adoption of a candidate cybersecurity certification scheme

Figure 5: European Cybersecurity Certification Scheme definition process

Even if the final purpose of the cyber security Act is to cover every topic at once, at the moment there are priorities on several sectors that are in needs of EU-wide certification. The main topics can be summarized in the following list:

- Common Criteria and SOG-IS MRA
- Cloud
- Industrial Automation and Control Systems
- IoT
- Software and system security lifecycle management

Their development could allow in the short term to resolve the definition of the certification schemes of different application environments in which these topics are the main actors.

In July 2020 ENISA published a candidate EU Cybersecurity certification scheme as successor of the SOG-IS. The EUCC Candidate Scheme is based on Common Criteria methodology and it is oriented to the cybersecurity certification for ICT products (Ref. [10])

[3] SCCG - Stakeholder Cybersecurity Certification Group, ECCG - European Cybersecurity Certification Group

Chapter 4 Cybersecurity certification scheme analysis

In the previous chapter we have defined the security as a process and introduced a particular process that can be associated to different situations that focus their attention on Cyber security. Moreover, we have briefly analysed the development of Certification Scheme and pointed our attention to European situation. Now to address the real purpose of this document we'll enter in a generic Certification schemes to analyse its structure with his processes and its actors.

4.1 Radiography of a Certification scheme

When we enter the plot of a certification scheme, we immediately realize how articulated its structure can be made up of processes, regulations and of course the respective actors.

So, let's try to draw up a list of the components that make up a generic certification scheme.

The first element that comes to mind is the set of rules that this certification must satisfy.

In most cases, these rules are contained within a "standard", which in turn, in order to function properly, must be able to take into account a large number of parameters.

Therefore, it is fundamental to frame on which argument the standard is to be focused and that is what is its area of applicability, but also what is its geographical area of applicability, which introduces the next element.

Which is the organization that manages the standard and what are the rules of management and therefore of its development, in fact with the continuous developments of the technological field it is not conceivable to use a static standard, but its dynamic management must be foreseen..

It is also essential to define what the standard intends to evaluate (products, services, infrastructures, people, etc.), how the evaluation process is structured, and which organization physically carries out the evaluation process.

We could go on for so long and then further ramify this path assuming to analyse for each identified element the possible certification schemes implied by it.

For this extent, an example above all could be the need for a particular certification by a person in order to be an actor within another certification process.

Just to highlight the number and complexity introduced for the certifications in the previous statements, without descending to an excessive level of detail of the possible categories, we indicate below, in tabular form, a non-exhaustive list of the certification schemes existing in the Cybersecurity field, as defined in a publication proposed by the European Cyber Security Organization (ECSO).

The following Table 3 lists the cybersecurity standards, schemes and guidelines for products and components.

	Standard / Scheme / Guideline	Body	Country / Industry	Link
Generic IT Products	Certification de Sécurité de Premier Niveau (CSPN)	ANSSI	France Generic	https://www.ssi.gouv.fr/administration/produits-certifies/cspn/les-procedures-formulaires-et-methodologies
	Commercial Product Assurance (CPA)	NCSC	UK Generic	https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa

	Common Criteria	Signatories of the CCRA Signatories of the SOG-IS	International Generic	https://www.commoncriteriaportal.org/ www.sogis.org
	European Privacy Seal	EuroPriSe	Europe Generic products, websites	https://www.european-privacy-seal.eu/EPS-en/Home
	National IT Evaluation Scheme (NITES)	CSA Singapore	Singapore General	https://www.csa.gov.sg/
	Software Improvement Group (SIG) Software Quality Model for Security	Software Improvement Group	The Netherlands General	https://www.sig.eu/insight/practical-model-rating-software-security
	UL Cybersecurity Assurance Program (UL 2900-1 / 2)	UL	USA	http://www.ul.com/cybersecurity/
	ULD Datenschutz-Gütesiegel	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein	Germany (Schleswig-Holstein)	https://www.datenschutzzentrum.de/guetesiegel/ (German only)
Products used in Industry 4.0 and ICS	ANSSI protection profiles for industrial systems	ANSSI	France	https://www.ssi.gouv.fr/guide/profils-de-protection-pour-les-systemes-industriels/
	ISA/IEC 62433 (Security for Industrial Automation and Control Systems)	ISA/IEC	International	https://webstore.iec.ch/searchform&q=62443
	IACS Cybersecurity Certification Framework (proposed)	JRC	Europe	https://erncip-project.jrc.ec.europa.eu/networks/tgs/european-iacs
	IEEE 1686 (Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities)	IEEE	International Power transmission	https://standards.ieee.org/findstds/standard/1686-2013.html
	IEEE C37.240 (Cybersecurity Requirements for Substation Automation,	IEEE	International Power transmission	https://standards.ieee.org/findstds/standard/C37.240-2014.html

	Protection, and Control Systems)			
	IEC 62351 (Power systems management and associated information exchange – Data and communications security)	IEC	IEC TC 57 series of protocols	http://www.iec.ch/search/?q=62351
Products used in telecom, media and content	GSMA Network Equipment Security Assurance Scheme	GSMA and 3GPP	International	http://www.3gpp.org/news-events/3gpp-news/1569-secam_for_3gpp_nodes
Products used in the payment industry	EMVCo Security Evaluation	EMVCo	International Payment cards	https://www.emvco.com/approvals.aspx?id=31
	Mastercard's Cybersecurity Standards	Mastercard	International Payment cards	https://www.mastercard.com
	PCI PTS HSM Security Requirements	PCI SSC	International HSMs used in the payment industry	https://www.pcisecuritystandards.org/
	PCI Payment Application Data Security Standard (PCI PA-DSS)	PCI SSC	International Payment applications	https://www.pcisecuritystandards.org/
	PCI PIN Transaction Security Point of Interaction Security (PCI PTS POI) Requirements	PCI SSC	International Payment point of interaction devices	https://www.pcisecuritystandards.org/
	VISA Ready	VISA	International Payment applications	https://partner.visa.com/site/programs/visa-ready.html
Cryptographic	ANSSI RGS	Agence nationale de la sécurité de	France	https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/liste-

		systèmes d'information		des-documents-constitutifs-du-rgs-v-2-0/
	ASD Cryptographic Evaluation	Australian Signals Directorate (ASD)	Australia	http://www.asd.gov.au/infosec/evaluations.htm
	CESG Assisted Products Scheme (CAPS)	NCSC	UK	https://www.ncsc.gov.uk/scheme/products-cesg-assisted-products-service
	FIPS 140-2	NIST	USA	http://csrc.nist.gov/groups/STM/cmvp/standards.html#02
	ISO/IEC 19790 (Security requirements for cryptographic modules)	ISO/IEC	International	https://www.iso.org/standard/52906.html
Web applications	OWASP Application Security Verification Standard (including OWASP Top Ten)	OWASP	International	https://www.owasp.org/index.php/Top_10_2013
	OWASP Testing Guide	OWASP	International	https://www.owasp.org/index.php/Category:OWASP_Testing_Project
IoT products	IoT Security Testing Framework	ICSA Labs	USA / International	https://www.icsalabs.com/technology-program/iot-testing
	IoT Device Cybersecurity Capability Core Baseline	NIST	USA	https://www.nist.gov/publications/iot-device-cybersecurity-capability-core-baseline
Other IT products	MIFARE Security Certification	NXP	International MIFARE products	https://www.mifare.net/en/about-mifare/certification/
	ISO/IEC 19792 (Security evaluation of biometrics)	ISO/IEC	International Biometric systems	https://www.iso.org/standard/51521.html

Table 3: Cybersecurity standards and schemes for products and components

The following Table 4 lists standards and schemes for cloud service providers.

	Standard / Scheme / Guideline	Body	Country/Industry	Link
Cloud service providers	ANSSI SecNumCloud	ANSSI	France	https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/
	Cloud Computing Compliance Controls Catalogue (C5)	Bundesamt für Sicherheit in der Informationstechnik (BSI)	Germany	https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/Compliance_Controls_Catalogue_node.html
	Cloud Security Alliance Cloud Controls Matrix	Cloud Security Alliance (CSA)	International	https://cloudsecurityalliance.org/group/cloud-controls-matrix/ https://cloudsecurityalliance.org/group/open-certification/#_downloads
	Code of Practice for Cloud Service Providers	Cloud Industry Forum	International	https://www.cloudindustryforum.org/content/code-practice-cloud-service-providers
	EuroCloud StarAudit Certification	EuroCloud	Europe (International)	https://staraudit.org/
	ISO/IEC 27017 (Code of practice for information security controls based on ISO/IEC 27002 for cloud services)	ISO/IEC	International	http://www.iso.org/iso/catalogue_detail?csnumber=43757
	ISO/IEC 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors)	ISO/IEC	International	http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498
	TüV Rheinland Cloud Security Certification	TüV Rheinland	International	http://www.tuv.com/en/corporate/business_customers/information_security_cw/strategic_information_security/cloud_security_certification/cloud_security_certification.html

Table 4: Cybersecurity standards and schemes for cloud service providers

Finally, the following Table 5 lists the cybersecurity standards and schemes for service providers and organisations.

	Standard / Scheme / Guideline	Body	Country/Industry	Link
Generic organisations	AEI Seal of Cybersecurity for Organisations	AEI	Spain	https://www.aeiciberseguridad.es/index.php/Sello_AEI_5.1.1
	CIS Critical Security Controls	Center for Internet Security (CIS)	International	https://www.cisecurity.org/
	Cyber Resilience Review	US-CERT	US	https://www.us-cert.gov/ccubedvp/assessments
	FINCSC – Finnish Cyber Security Certificate	JAMK University of Applied Sciences and partners	Finland	https://www.fincsc.fi/ (Finnish only)
	ISF Standard of Good Practice for Information Security	Information Security Forum	International	https://www.securityforum.org/tool/the-isf-standardrmation-security/
	IT Grundschutz	Bundesamt für Sicherheit in der Informationstechnik (BSI)	Germany	https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html
	ISO/IEC 27001 (Information Security Management Systems – Requirements)	ISO/IEC	International	http://www.iso.org/iso/iso27001 http://www.iso.org/iso/catalogue_detail?csnumber=54534
	ISO/IEC 27032 (Guidelines for cybersecurity)	ISO/IEC	International	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44375
	ISO/IEC 27033 (Network security)	ISO/IEC	International	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63461
	ISO/IEC 27034 (Application security)	ISO/IEC	International	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44378

	Standard / Scheme / Guideline	Body	Country/Industry	Link
	ISO/IEC 27035 (Information security incident management)	ISO/IEC	International	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62071
	ISO/IEC 27036 (Information security for supplier relationships)	ISO/IEC	International	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59648
	ISO/IEC 29100 (Privacy architecture framework) and related ISO standards	ISO/IEC	International	https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en
	LEET Security Stamp	LEET Security	Spain	http://www.leetsecurity.com/
	Open Trusted Technology Provider Standard (O-TTPS) & ISO/IEC 20243 (O-TTPS -- Mitigating maliciously tainted and counterfeit products)	Open Group ISO/IEC	International	https://www2.opengroup.org/ogsys/catalog/c139 http://www.opengroup.org/certifications/o-ttps http://www.iso.org/iso/catalogue_detail.htm?csnumber=67394
	Service Organisation Control (SOC)	AICPA	USA General	http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/ServiceOrganisation%27sManagement.aspx
	Shared Assessments Program	Shared Assessment	International Vendor management	https://sharedassessments.org/about/
	ULD Datenschutzaudit	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein	Germany (Schleswig-Holstein)	https://www.datenschutzzentrum.de/audit/ (German only)
Industry 4.0 and ICS	ANSSI Cybersecurity for Industrial Control Systems	ANSSI	France General ICS	https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf https://www.ssi.gouv.fr/uploads/2014/01/industrial_s

	Standard / Scheme / Guideline	Body	Country/Industry	Link
				ecurity_WG_detailed_measures.pdf
	ANSSI protection profiles for industrial systems	ANSSI	France ICS equipment and software	https://www.ssi.gouv.fr/guide/profils-de-protection-pour-les-systemes-industriels/
	API STD 1164 (Pipeline SCADA Security)	American Petroleum Institute (API)	USA Oil and Gas	https://global.ihs.com/doc_detail.cfm?document_name=API%20STD%201164
	BSI ICS Security Compendium	Bundesamt für Sicherheit in der Informationstechnik (BSI)	Germany General ICS	https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/ICS-Security_compendium.html
	Catalog of Control Systems Security	Department of Homeland Security (DHS)	USA General ICS	https://ics-cert.us-cert.gov/sites/default/files/documents/CatalogofRecommendationsVer7.pdf
	ICS-CERT assessments: • CSET • DAR • NAVV	ICS-CERT	USA General ICS	https://ics-cert.us-cert.gov/Assessments
	ISA/IEC 62433 (Security for Industrial Automation and Control Systems)	ISA/IEC	International General ICS	https://webstore.iec.ch/searchform&q=62443 http://www.isasecure.org/en-US/
	NIST SP 800-82 (Guide to Industrial Control Systems (ICS) Security)	NIST	USA General ICS	http://dx.doi.org/10.6028/NIST.SP.800-82r2
Energy and smart grids	Cybersecurity Capability Maturity Model	US Department of Energy	US Energy, Electricity, Oil and Gas	https://energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturity-model-c2m2-program
	ISO/IEC 27019 (Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry)	ISO/IEC	International General energy systems	https://www.iso.org/standard/43759.html

	Standard / Scheme / Guideline	Body	Country/Industry	Link
	NERC Critical Infrastructures Protection (CIP) standards 002 - 009	NERC	USA Electrical Grid	http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
	NIST IR 7628 (Guidelines for Smart Grid Cybersecurity)	NIST	USA Smart grids	https://www.nist.gov/node/562431
Transportation (road, rail, air, sea)	EUROCAE ED-202A (Airworthiness Security Process Specification)	EUROCAE	Europe Aviation	https://standards.globalspec.com/std/9862360/eurocae-ed-202
	RTCA DO-326A (Airworthiness Security Process Specification)	RTCA	USA Aviation	http://www.rtca.org/store_product.asp?prodid=1173
	ISO-SAE 21434 (Road Vehicles – Cybersecurity Engineering)	ISO / SAE	International Vehicles	https://www.iso.org/standard/70918.html
	SAE J3061 (Cybersecurity Guidebook for Cyber-Physical Vehicle Systems)	SAE	International Vehicles	http://webstore.ansi.org/RecordDetail.aspx?sku=SAE+J+3061-2016+(SAE+J3061-2016)
	The Guidelines on Cyber Security onboard Ships	BIMCO et al.	International Shipping	http://www.srhmar.com/images/stories/pdf/Guidelines_on_cyber_security_onboard_ships.pdf
Financial services and insurance	BITS Software Assurance Framework	BITS	International Software development	http://fsroundtable.org/bits/about-bits/
	CBEST	Bank of England	UK Financial service providers	http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx#
	ISO/IEC 27015 (Information security management guidelines for financial services)	ISO/IEC	International Financial service providers	https://www.iso.org/standard/43755.html

	Standard / Scheme / Guideline	Body	Country/Industry	Link
Public services / eGovernment / Digital Citizenship	Application Security and Development Security Technical Implementation Guide (STIG)	DISA	USA Federal IT systems	http://iase.disa.mil/stigs/app-security/app-security/Pages/index.aspx
	ISKE	Administration system for the state information system (RIHA)	Estonia State and local governments handling databases or registers	https://www.ria.ee/en/iske-en.html
	National Security Framework (Esquema Nacional de Seguridad - ENS)	Entidad Nacional de Acreditación	Spain Public sector organisations and their service providers	https://administracionelectronica.gob.es/ctt/verPestanaGeneral.htm?idIniciativa=ens&idioma=en#.WNpAE7u7r4Z
	NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organisations)	NIST	USA Federal IT systems	https://web.nvd.nist.gov/view/800-53/Rev4/home
	Guidelines on ICT and security risk management	EBA (European Banking Authority)	International	https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management
Healthcare	ISO/IEC 27799 (Health informatics - Information security management in health using ISO/IEC 27002)	ISO/IEC	International	https://www.iso.org/standard/62777.html
	ISO/IEC 62304 (Medical device software – Software life cycle processes)	ISO/IEC	International Medical software development	http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=71604
	IT Health CHECK Service (CHECK)	National Centre for Cyber Security (NCSC)	UK Healthcare providers	https://www.ncsc.gov.uk/articles/check-fundamental-principles

	Standard / Scheme / Guideline	Body	Country/Industry	Link
Smart cities and smart buildings	ISA/IEC 62433 (Security for Industrial Automation and Control Systems)	ISA/IEC	International General ICS	https://webstore.iec.ch/searchform&q=62443 http://www.isasecure.org/en-US/
Telecom, media and content	GSMA Security Accreditation Scheme	GSMA	International UICC providers	http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme
	ISO/IEC 27011 (Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organisations)	ISO/IEC	International	https://www.iso.org/standard/64143.html
	TL 9000 Quality Management System	QuEST Forum	International ICT vendors	http://www.tl9000.org/
Critical infrastructures	AEI Seal of Cybersecurity for Organisations	AEI	Spain General	https://www.aeiciberseguridad.es/index.php/Sello_AEI
	KRITIS	Bundesamt für Sicherheit in der Informationstechnik (BSI)	Germany General	http://www.kritis.bund.de/SubSites/Kritis/DE/Publikationen/publikationen_node.html
	NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework)	NIST	USA General	https://www.nist.gov/cyberframework
	Référentiel Général de Sécurité (RGS)	ANSSI	France General	https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/ (French only)

	Standard / Scheme / Guideline	Body	Country/Industry	Link
General secure software development	BSI PAS 754 (Software trustworthiness – Governance and management – Specification)	British Standards Institution (BSI)	UK	http://shop.bsigroup.com/ProductDetail/?pid=000000000030284608
	Building Security in Maturity Model (BSIMM)	Gary McGraw, Sammy Migues, and Jacob West	International	https://www.bsimm.com/
	ISO/IEC 21827 (Systems Security Engineering - Capability Maturity Model)	ISO/IEC	International	https://www.iso.org/standard/44716.html
	Microsoft Security Development Lifecycle	Microsoft	International	https://www.microsoft.com/en-us/sdl/
	OWASP Software Assurance Maturity Model	OWASP	International	https://www.owasp.org/index.php/OWASP_SAMM_Project http://www.opensamm.org/
Cybersecurity service providers	ANSSI requirements for security service providers (PDIS, PRIS, PASSI, PSCE, PSHE)	ANSSI	France Service providers for • Incident detection • Incident response • Information system security auditing • Electronic certificates • Electronic timestamping	https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/
	CREST Simulated Targeted Attack and Response (STAR)	Council for Registered Ethical Security Testers (CREST)	UK	http://www.crest-approved.org/uk/what-we-do/index.html

	Standard / Scheme / Guideline	Body	Country/Industry	Link
Payment industry	PCI Data Security Standard	PCI SSC	International Card Payments	https://www.pcisecuritystandards.org/
IoT device vendors	BITAG Internet of Things (IoT) Security and Privacy Recommendations	BITAG	International General	https://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php
	Future-proofing the Connected World	Cloud Security Alliance IoT Working Group	International General	https://cloudsecurityalliance.org/download/future-proofing-the-connected-world/
	GSMA IoT Security Guidelines	GSMA	Internal Telecom	http://www.gsma.com/connectedliving/gsma-iot-security-guidelines-complete-document-set/
	Industrial Internet of Things Security Framework	Industrial Internet Consortium	International Industrial IoT systems	http://www.iiconsortium.org/IISF.htm
	IoT Security Compliance Framework	IoT Security Foundation	International General	https://iotsecurityfoundation.org/best-practice-guidelines/
	Online Trust Alliance IoT Trust Framework	Online Trust Alliance	USA General	https://otalliance.org/resources/iot-industry-resources
	OWASP Internet of Things Project	OWASP	International General	https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
	Strategic Principles for Securing the Internet of Things (IoT)	Department of Homeland Security	USA General	https://www.dhs.gov/securingtheIoT

Table 5: Cybersecurity standards and schemes for service providers and organisations

In a perfect world vision, all these standards and schemes, aggregated for example by group, could refer to each other to ensure that no element of a global process (see also section 2.3 of this document and Chapter 6) is neglected from the point of view of cybersecurity, and it could be a definitive solution.

In order to reach this perfect world vision, it is needed to walk a long road by creating a link between all these standard/scheme/guidelines. This cannot be achieved in the near future because there is the need to establish a roadmap that defines formally how these links can be created. The first step could be improving the existing network of collaboration between the certification bodies. The following sections try to indicate in an exhaustive way the steps that lead us to introduce the topic of task 11.3, the "evaluation laboratory", to understand later, in the rest of this document, how, in a larger project they can evolve. In the following a generic cybersecurity certification scheme is used.

4.2 Process and actors of a Cybersecurity certification scheme

As observed when it comes to certification schemes, there is a huge number of applicable standards connected to an equally vast geographical applicability.

Let us now go into detail on the certification process in which these elements are involved, naturally also introducing the actors of this process.

Going to focus our attention on the cybersecurity certification of product, system or process (topic of this project), we have that above all it arises as a requirement in a certain context which:

- can derive from a particular interest (response to legislation, a market need, etc.)
- can be limited geographically or not (national, international context, but also by product sector, for a professional profile, etc.)

in order to provide an estimate of the security level according to a certain standard, shared by all the involved subjects, and to ensure that this estimate is performed by a third party independent from the subjects themselves.

Afterwards the primary need for a Certification Body (CB) arises, which has the task of managing the entire scheme through two distinct phases:

- a first phase of an implementing nature: in which it prepares a series of elements that will characterize the scheme, such as the technical rules on certification on the basis of the contextual needs (the interest and limitations previously mentioned) and the evaluation and certification processes.
- a second phase of an operational nature: in which it will oversee all the evaluation and certification operating activities within the framework.

Certification bodies have not to be confused with Accreditation bodies (see section 4.2.2)

Naturally, the aforementioned processes relating to the scheme must be observed by all those entities (natural persons, legal entities and any other body or association) which are responsible for decisions regarding the request, acquisition, design, implementation, installation and use of products, systems and processes that need a security certification in compliance with international standards.

Currently, the certification body must also manage any international mutual recognition agreements for certifications, which also deal with the application, harmonization and evolution of the standard adopted in a wider context. However, if we refer to what is indicated in the Cyber Security Act (par. 3.2), the schemes that will be defined will be valid throughout the European context.

To complete the framework, the actors, who under the direction of the Certification Body are involved in the evaluation and certification process within the scheme must be introduced. By using the terminology of Common Criteria, the necessary involved in a certification process are:

- Sponsor.
- Developer.
- Cyber Security Evaluation Facility (CSEF).

moreover, an optional figure depending on the situation, that is represented by the Consultant.

In the following let us try to go deeper into the role and tasks assigned to each previously identified actor.

4.2.1 Certification Body (CB)

It certainly represents the leading role and as such a certification scheme should enable only one Certification Body (CB), even if today there are situations in which there are schemes in which, for the same type of certification, there are multiple Certification Bodies.

The CB must supervise all the operational activities of evaluation and certification within the scheme through a series of actions that can be summarized as follows:

- prepare the technical rules on certification on the basis of reference standards and directives.
- disclose the principles and procedures relating to the Scheme.
- coordinate the activities under the scheme consistently with defined evaluation criteria and methods.
- prepare guidelines for the evaluation process inside the scheme.
- manage the Cybersecurity Evaluation Facilities through:
  - their accreditation, suspension and revocation.
  - verification of the maintenance of independence, impartiality, reliability, technical skills and operational capabilities of accredited CSEFs.
  - preparation, updating and publication of the list of accredited CSEFs.
- manage the individual Evaluation Processes through:
  - approval of an evaluation plan
  - registration of the evaluation process in the scheme.
  - approval of the Evaluation Technical Reports.
- manage the Certification Reports: issue and revocation.
- manage the list of products, systems, processes certified and being certified: definition, updating and publication
- promote activities for the dissemination of the culture of security in the information technology sector.
- manage the training and training of the Certifiers, employees of the OC.
- carry out the training of the Evaluators, members of the CSEF, and of the consultants.
- manage the list of Evaluators and consultants (definition, updating and publication).

4.2.2 Accreditation Body

An Accreditation Body (AB) is an independent organisation responsible for assessing the performance of other organisations against a recognised standard, and for formally confirming the status of those that meet the standard.

In cybersecurity schemes, accreditation might be required by the scheme owners against:

- ISO 17025 for evaluation facilities,
- ISO 17065 for certification bodies.

In Europe, accreditation has to abide by the regulation n° 765/2008 (Ref. [18]).

4.2.3 Cyber Security Evaluation Facility (CSEF)

As previously defined, during the evaluation activity the Certification Body relies on CSEFs, which carry out the activities related to the evaluation and which must be accredited by the CB itself.

For the purpose of such accreditation, CSEF must possess very specific requirements defined by the Certification Body within the certification scheme.

Of course, the laboratory must maintain these requirements over time.

In addition to Evaluation activities, a CSEF can also carry out the activities listed below:

- Advice to the Sponsor on the evaluation / certification process through:
  - training activities on the processes involved.

  - preparing of the documentation needed for the evaluation purpose during the preparation and/or conduction of the Evaluation process.
  - determination of the evaluability of the product, system or process.
  - the activities connected with the management and maintenance of the Certificates.
- Training on security issues in the information technology sector in general and, in particular, on evaluation processes.

CSEF is required to give prior notice to the CB every time it performs one of the aforementioned activities and of course if one or more Consultants of a CSEF give assistance to a Sponsor or a Developer for a product, system or process or part of it, they cannot participate to the evaluation of the same.

4.2.4 Sponsor

The Sponsor is the natural/legal person or any other body that commissions Evaluation and can coincide with developer role.

It is up to the Sponsor to choose the CSEF and to request to the Certification Body the registration of the Evaluation process in the scheme.

4.2.5 Developer

The Developer is the natural/legal person or any other body that supplies the product, system or process to be certified, or a component part of the same.

As introduced in the previous paragraph, the Developer can also play the role of Sponsor of the evaluation process.

In the event that the Sponsor is not also the Developer, it will be necessary for the latter to be available to cooperate with the Sponsor in the evaluation and certification process, providing the technical information and documentation, in its possession, required for the evaluation.

4.2.6 Consultant

The consultant can be a single person or a group of people trained and authorized by the CB to provide technical support to a Sponsor/Developer, or a CSEF who requests it (for example to produce the documentation necessary for the evaluation process, to estimate the probability of success of the certification process, etc.).

4.2.7 Cybersecurity evaluation/certification process and CSEF involvement

Once the actors have been defined, it is possible to hypothesize how they act within a generic certification process, focusing on the role that the Cybersecurity Evaluation Facility (CSEF) assumes during the evaluation process

The evaluation process conducted within a generic Scheme can be divided into three phases:

- Preparation
- Conduct
- Conclusion

In these phases it is necessary to define a certain number of procedures that characterize them and which can be summarized as follows:

- communications between Cybersecurity Evaluation Facility, Sponsor, Developer and Certification Body (CB).
- the organization and planning of evaluation activities.
- checks for the evaluation activities.
- the publication of the results of a certification.

Let's see in summary these phases, which will be deepened below.

The preparation phase involves the Sponsor, Developer and the CSEF, which examines the documentation related to the Target of the Evaluation (TOE) and produces an Evaluation Plan (EP), detailing how the evaluation should be carried out.

The CSEF also produce a list of materials for the evaluation, identifying the necessary documentation and any support requested from the TOE Sponsor/Developer.

Before defining a contractual relationship, the Sponsor/Developer and the CSEF may contact the CB to verify any problems in carrying out the evaluation under the defined scheme.

Once the agreement between CSEF and the Sponsor/Developer has been defined, the they must submit to the CB the request for formal registration of the evaluation in the Scheme, attaching the Toe description and the Evaluation Plan prepared by the designated CSEF.

The conducting phase begins when the CB, having examined the material received, approves the Evaluation Plan and formally accepts the evaluation process in the Scheme.

In the conclusion phase, the CSEF produces an Evaluation Technical Report (ETR) which summarizes all the results obtained during the evaluation and which is used by the CB as a basis for the preparation of the Certification Report.

More details on the individual phases are provided in the following paragraphs.

4.2.7.1 Preparation

The objectives of this phase are:

- determine the adequacy of the product, system or process for evaluation (TOE) by analyzing the materials made available by the Developer
- produce an Evaluation Plan (document containing the description of the activities envisaged for the evaluation process, providing sufficient details to be able to estimate the progress of the evaluation process for each foreseen activity) and a list of materials for the evaluation (any hardware elements, firmware or software that are the target of the assessment and the supporting technical documentation to permit the evaluation process;

The Sponsor/Developer identifies a CSEF for carrying out the assessment activities, to which it delivers a descriptive document of the TOE

The Sponsor/Developer can also request assistance from the CSEF, as mentioned in section 4.2.6.

Once the CSEF has carried out the checks indicated in a) and produced the document defined in b), the Sponsor/Developer submits an official request to the CB for registration in the proposed certification scheme by attaching the necessary documentation.

Upon receipt of the request, the CB examines the attached documentation and in particular, the Evaluation Plan in order to also verify the adequacy of the resources and timescales provided by the CSEF for conducting the evaluation process.

Once the suitability is established, the CB communicates this decision simultaneously to the Sponsor/Developer and the CSEF, which can then start the evaluation activities.

4.2.7.2 Conduct

This phase forms the core of the evaluation process and is performed almost completely by the CSEF with the participation of the other actors. The goal is to:

- demonstrate that the activity was carried out in compliance with the reference standard and the contents of the Evaluation Plan
- demonstrate that the activity was carried out objectively and impartially.
- the results are repeatable and reproducible.
- provide sufficient evidence from the Evaluators to justify the resulting conclusions.

This phase begins with a start-up Meeting between the actors of the process.

During the evaluation, if the Evaluators detect problems relating to the evaluation target, they produce Observation Reports (OR).

Once the actions and countermeasures proposed for the resolution of the problem have been identified, the Developer must issue the response to the OR, which will be sent simultaneously to the CSEF and the CB.

If, on the other hand, the solution of the problem involves more relevant actions (such as modifications of the TOE), the OC will call a specific Evaluation Control Meeting, in which the CSEF and the Sponsor (and possibly the Developer) will participate to verify the feasibility and the opportunity of the requested actions.

At the end of each partial activity of the evaluation process, the CSEF prepares an Activity Reports (AR) which summarize the results of the conducted analysis on that specific activity. These reports are normally sent to the CB at the end of each activity. In relation to the content of the ARs, the CB decides on the opportunity to transmit them to the Sponsor/Developer.

For assessments that are not particularly complex, ARs can be produced at the end of the assessment.

4.2.7.3 Conclusion

In the conclusion phase, the CSEF produces an Evaluation Technical Report (ETR) which reports the verdicts and considerations made by the Evaluators. It is sent exclusively to the CB, which revises it to check that it provides an adequate summary of the evaluation results.

If this revision is successful, the ETR is approved. In the event of a positive evaluation of the Target by CSEF, the ETR is used by the CB as a basis for the production of the Certification Report that accompanies the related Certificate, that is the attestation that the Target has been evaluated by an accredited CSEF in accordance with the evaluation criteria indicated by the reference standards and with the Scheme procedures.

The role of the CSEF during the certification phase is to provide technical support to the CB in the revision of the ETR and in the production of the Certification Report. For example, this support could involve the Evaluators in:

- provide access to specific technical demonstrations (for example evaluation materials, results obtained from the use of specific tools) to support their conclusions.
- providing clarifications on the contents of an AR or the ETR.
- participate in a technical review committee / commission, called if considered necessary by the CB (for example if the results of an AR are not clear);
- review the Certification Report to ensure that it is technically accurate and consistent with ETR.

Chapter 5 Security Evaluation Facility – Today and tomorrow

5.1 Analysis of the Security Evaluation Facilities for the various reference standards in the European context

5.1.1 High security assurance: context for SEF active in Common Criteria (CC), FIPS, and derivate schemes

In order to identify the specificities of the CC context, it is useful to start from a comparison between the Common Criteria and their great global competitor as the reference security scheme, which is FIPS 140.

Historically, the FIPS and Common Criteria schemes have been instrumental in building the CSEF landscape. Quite often, the laboratories involved in high security assurance ("ITSEFs" in Europe, from the CC and SOG-IS schemes) will be active in the two schemes, as well as in the numerous schemes that derive from one or the other.

In the comparison between FIPS and Common Criteria:

- There are similarities between the two schemes:
- The evaluation facilities are third-party laboratories, independent from the Certification Bodies.
- The certification Bodies are either government agencies, or private agencies operating under government delegation.
- The evaluation facilities shall be accredited according to ISO/IEC 17025;
- The evaluation facilities shall be licensed by the Certification Bodies.

However, there are quite different approaches between the US landscape, mainly focused on FIPS, and the European landscape, where Common Criteria has a huge influence.

The difference relies mainly on the role played by vulnerability analysis (and associated pen-testing tasks). Vulnerability analysis is essential in Common Criteria as well as the numerous schemes inspired by the CC – most of these schemes will even focus on vulnerability analysis and give up on conformity tasks. EMVCo is one of these schemes; the focus on AVA_VAN related tasks being mainly possible because these schemes will be derivate from CC to address the needs of a specific class of products, such as banking products for EMVCo, so that all conformity analysis will be simplified because of commonality throughout the certified products.

On the contrary, FIPS will focus on conformance to functional security requirements, and test suites dedicated to checking that the functional security requirements are met.

In the field of physical security, the difference of approach is well documented by e.g.[6]. Side-Channel Analysis is an important part of any security evaluation for hardware security products. The FIPS standard will focus on leakage assessment through normalized tests and statistical methods, while the Common Criteria laboratories will perform the whole attacks according to their state of the art.

So, there is a very clear difference in the approaches, as well as in the certification procedures.

There are reasons to argue that vulnerability analysis is essential in security evaluation. Basically, it accounts for the fact that in cybersecurity the threat is a malevolent, knowledgeable, focused human entity. So, the evaluation schemes should let the evaluator analyse the Target of Evaluation, and incorporate evolving attack techniques, to devise personalized tests, just like the attacker will do "on the field".

However, there are pros and cons. The higher security assurance provided by Common Criteria comes at the following constraints:

1. Need to ensure that the ITSEFs are up to state of the art,
2. Need to ensure that similar evaluation projects conducted by different ITSEFs under the supervision of the same CB would lead to similar results,
3. Need to ensure consistency of the certificates delivered for similar products from one CC scheme to another,
4. Lengthy evaluations because of the need to account for all possibly relevant attack paths,
5. Need to account for the practical difficulties implied by management of confidential customer data (the CC Whitebox approach is necessary not only to limit the time spent by the evaluator in analysing the TOE, but also to minimize the risk of "missing" a vulnerability of the product design) as well as careful handling of attack methods that might be used by wrong-doers if disseminated.

The organization of the CC schemes and the relationships between ITSEFs, CBs and developers are based on how to handle these constraints.

5.1.2 Organization for Common Criteria certification

5.1.2.1 Relationship between the CBs and the ITSEFs

The ITSEF are in close relationship with their national CBs. Apart from normal 17065-like duties of any certification body, the following CC peculiarities are worth highlighting:

- the CC CBs are also responsible for assessing the skills and knowledge of the ITSEF they work with. This task is related with constraints 1 and 2. This goal is met through various means:
    - technical audits of the laboratories, which may result in the loss of the license to perform such or such work units for CC evaluations.
    - production of technical notes for the ITSEFs based on field returns, bibliography, interpretation of standards, information shared by other schemes;
    - "animation" of the scheme, which may include regular meetings between the labs and the CB, technical challenges, common technical writing etc.
- The CBs monitor the different stages of evaluations. In preparation phase they will review the evaluation plan, including the estimated workload to ensure that it is sufficient (the economic burden of constraint 4 is mitigated by the competition between the ITSEF, but the CB will check that the resulting workload still ensures that the work will be complete). During the evaluation, they will hold regular reviews with the evaluator and the sponsor of the evaluation.
- With regards to constraint 5, the CBs may define security requirements to be met by the ITSEFs, and the National Accreditation Bodies may check that these requirements are met during the site audits. (Constraint 5 is also addressed through NDAs between the evaluation sponsor and the ITSEF).

5.1.2.2 Relationship between the different CC schemes

Constraint 3 on the need to ensure consistency of the certificates delivered by different national schemes, in the optic of mutual recognition agreements, has at least two justifications:

- It is a way to mitigate the economic consequences of constraint 4: it is neither affordable nor time-efficient to undergo different evaluations in different countries,
- And it is necessary to ensure the success of the CC scheme compared to other private, global security schemes, especially with regards to a globalized ICT market.

In order to meet this constraint, different countries have entered mutual recognition agreements with specific mechanisms.

The Common Criteria Recognition Arrangement (https://commoncriteriaportal.org/ccra/) gathers countries which agreed to officially recognize the participants' certificates up to EAL2 (or EAL4 in the case of common Protection Profiles). This arrangement includes such peer assessment mechanisms as "voluntary periodic assessments" or "shadow certifications".

The SOG-IS MRA agreement (https://www.sogis.eu/uk/supporting_doc_en.html) has a more European footprint and most importantly it extends the security assurance level mutually recognized:

- Up to EAL4 in all cases,
- Up to EAL7 for evaluations performed by some of the evaluation facilities, in two technical domains which are "smartcards and similar devices" (at silicon level, a secure element is an example of such similar device; passports, ID cards are other such items) on one hand and "hardware devices with security boxes" (HSM for example).

In accordance with the high level of mutual trust in the certificates delivered by the participants, the SOG-IS MRA includes conditions for recognition in terms of scheme organization, quality assurance, content of the certificates and of the certificate reports, share of information (sets of schemes' rules and regulations, certificates and certificate reports, etc). Also "voluntary" periodic assessments are performed with a goal at maximum intervals of five years. The CBs will audit one another, and their associated ITSEFs may be involved in these audits.

Overall CC scheme animation

Sharing information is identified as a goal in the mutual recognition agreements. This involves:

- sharing information between national CC schemes,
- engaging with stakeholders on a need-to-know basis through working groups such as ISCI WG1 or ISCI WG2 ("JHAS" and "JEDS" gather CBs, laboratories and developers to discuss attack methods to be applied respectively for "smartcard and similar devices" and "hardware devices with security boxes")
- holding international conferences such as ICCC.

All in all, this organization has ensured that the Common Criteria environment has been providing the reference security scheme (especially for security products) for more than twenty years.

5.2 Perspectives for the Security Evaluation Facilities evolution

5.2.1 Laboratory tools and organization

5.2.1.1 Laboratory organization

The CSA Group focus on IEC/ISO 17065 norm for CABs (Conformity Assessment Bodies) as well as the inheritance from CC, EMVCo, FIDO schemes should lead the Security Evaluation Facilities to abide by the general organization required by the ISO/IEC 17025. Therefore, laboratories will have to:

- be legally responsible entities, or part of a legally responsible entities,
- able to demonstrate that they are protected from any conflict of interest that may hamper their impartiality both externally with regards to the remainder of the entities they may be part of, and internally with regards to any undue commercial, financial, contractual… pressure that the evaluators may be subjected to. For example, the laboratory should not engage in any activity that may put its impartiality at odds: so consultancy activities should be clearly segregated from evaluation activities. This is, and will remain a matter of specific importance and vigilance for the managers of laboratories that are active in the field of cybersecurity, because human resources are scarce compared to the needs, and the very high expertise of these evaluation laboratories would put them in a very good position to provide useful insights to the developers.
- Be able to protect the confidential information related to the products and IP of their customers, all the more so in cybersecurity because of the "white box" principle and because leaked sensitive information may be useful to third party attackers
- Name staff members responsible for technical management, equipment, and quality and name substitute people responsible for these tasks.

Apart from these general principles that will probably last, the organizations are likely to evolve along the following lines:

- Bigger laboratories should be expected. Compared to the small laboratories which are the historical trend, bigger ones will appear and are already appearing, with the help of the following factors: ever-increasing need for security certification, and needs to limit the price of the certification, can be partly solved by bigger structures with reproducible means of evaluation. Also, the CSA focus on private CABs with their internal evaluation facilities reinforces the interest of the cybersecurity market for such certification firms as Bureau Veritas, SGS, TÜV… that will be able to attain vertical integration of evaluation and certification activities.
- Niche markets will remain for small, expert laboratories, especially at “HIGH” (EAL4 and beyond, and more notably around AVA_VAN.5) where the focus will be on expert vulnerability analysis, conducted under overall supervision from public CABs and NCCAs

5.2.1.2 Laboratory tools

The quest for pen-test automation will remain a driver, especially for software attacks (misuse and abuse, fuzzing). This is a way to limit the need for highly skilled evaluators, accelerate the time needed for evaluation, and increase the test coverage. However, vulnerability analysis cannot be fully automated, and such tools should only be seen as helping the human evaluator.

Complementary software help tools will be used for formal evaluation and code analysis, with the support of strong, on-going R&D activity especially from ITSEFs, research and technology offices (such as CEA List or INRIA in France) or specialized SMEs.

Physical semi-intrusive or intrusive attacks will continue to enjoy the current trend of incremental improvement. Still it is likely that specific developments will be needed on the low and high limits of the test benches:

- At low limit, specific effort should be conducted for ITSEFs to take into account the cheapest means of attacks that may be accessible to expert users (the CC document “Application of Attack Potential to Smartcard”, version 2.4, June 2021, puts the emphasis on individual equipment cheaper than 10 k€)

- At high limit, either new equipment will be needed to address the latest, tiniest technological nodes, or currently achievable attacks (e.g., circuit edit by means of a high-end Focused Ion Beam) will no longer be practical.

These two trends will be hardly addressed by individual security evaluation facilities according to their current organization. At low limit, it will require redundant equipment and expertise, whereas at high limit it will involve high R&D effort and use of ever-more expensive equipment which may not prove adequate (and therefore worthwhile investments) for the ensuing evaluation projects: there is no use in trying attacks which are deemed impractical after *a priori* vulnerability analysis.

Chapter 6 A Perfect World Vision

In this chapter, let us start to analyse an existing laboratories network in order to find some improvement that could lead to a “perfect world vision”.

Typically, when a product under certification interacts with or make uses of other certified products, the evaluation laboratory cannot go deeper in the security analysis of the already certified product and/or it cannot re-use evidences and/or assurance activities produced during other certification having a similar scope.

This happens because concerned information is typically subject to NDA (Non-Disclosure Agreement) between the developer, the sponsor, the laboratory and the Certification Body.

When publicly available, the CSEF can access to Certification Report or some other public documents of the certified product (if we talk about Common Criteria typically the Security Targets and Guidance Documentation are publicly available) in order to use them as support documents during the evaluation.

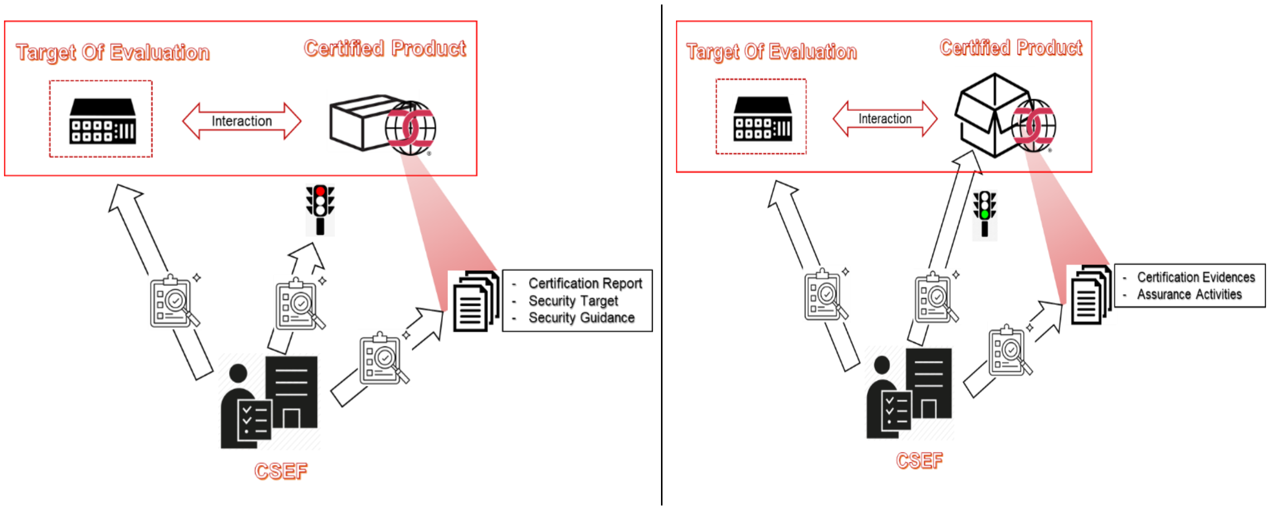


Figure 6: “Black box” and “White box” Security Certification

The principle is that a laboratory does not need to have more information on a certified product because the certification schema ensures that the certified product reached successfully the defined security objectives and the targeted assurance level (Black box approach on the left in Figure 6).

The Certification Body guarantees the results provided by CSEFs (by issuing the Certification Report) during the evaluation and this information can be considered sufficient for performing a new evaluation with other products that interact with certified products.

However, typically, the constraints are that the certified products have to be used in their certified configuration (version, configurations, etc.).

The boundaries of the certified product have to be guaranteed and in line with the obtained certification if the boundaries, configurations, interfaces, are guaranteed.

But what happened when during the evaluation of a new product interacting with a certified product there is the need to modify its configuration?

The problem can be traced back to the problem of the maintenance of the certification.

With the same principle of Assurance Continuity, an impact analysis on the certified products should be performed in order to guarantee the certificate maintenance of the “modified” certified product.

In a perfect world vision, the sharing of evidences and assurance activities between CSEFs and Certification Bodies could help improving the overall security and help having faster certifications (White box approach on the right of Figure 6).

For example, the change of some configurations to an already certified product could be evaluated by the CSEF during the new certification and, in case of minor changes; the products could quickly maintain the certification. In this way, also the new configuration could be used as a new evaluated configuration of the product.

Moreover, laboratories, having the possibility to access some more detailed information of certified products could perform a certification with an improvement of overall security in particular in the interactions between the product under certification and certified products.

This could be very useful in case of certification of more complex systems where the TOE is supported in its operational environment objectives by a complex environment constituted by some certified products.

Let us imagine the following cases:

- a certification of a web application that relies on a set of security functionalities provided by the Operating Systems, the application server, the database, the hypervisor, etc.
- a Complex System designed and developed in order to rely on set of certified products

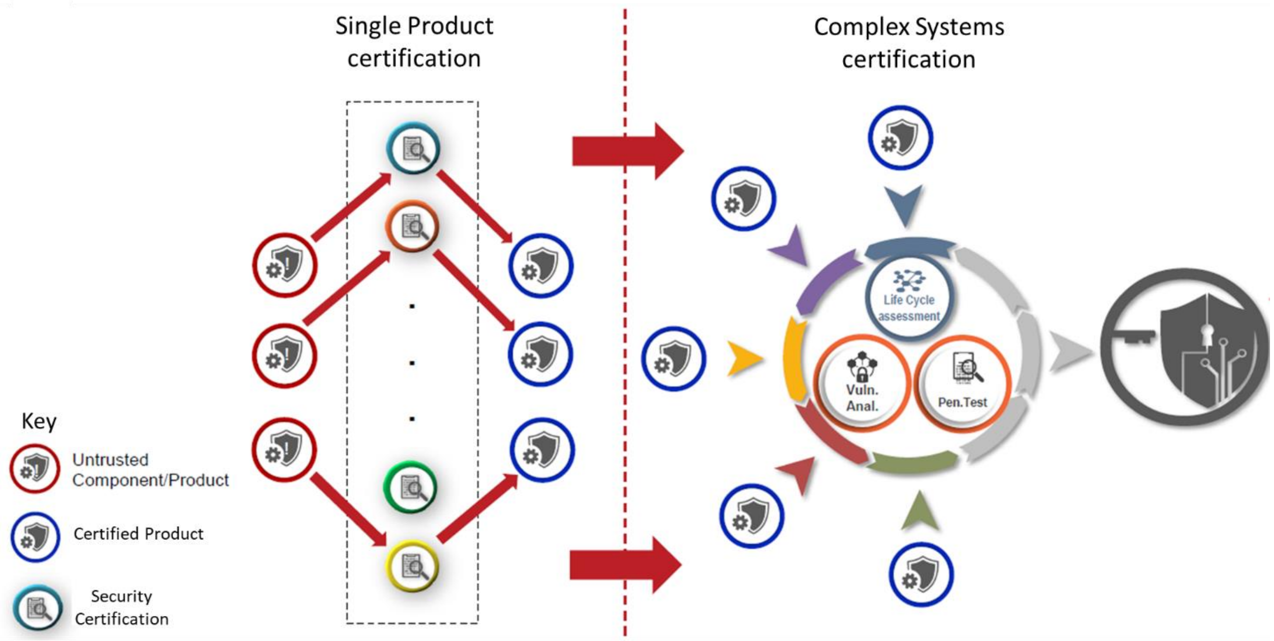

Single Product certification
Complex Systems certification
Key
Untrusted Component/Product
Certified Product
Security Certification
Life Cycle assessment
Vuln. Anal.
Pen.Test

Figure 7: Single Product certification re-used for Complex Systems certification

In these cases, the complex systems certification could be faster and simpler focusing on specific activities like Vulnerability Analysis, Penetration Testing and Life-Cycle Management.

Other evidences could be formally available by re-using evidences and assurance activities performed for the certification of single products (on the left in Figure 7).

Finally, having an improved network of collaboration, including a faster information sharing, could lead to make faster certification of similar products because the laboratories could exchange more detailed information on activities performed by other laboratories.

In a perfect world vision, the objective is working to formalize a way for improving the existing interactions between the laboratories and Certification Bodies improving and defining rules about information sharing of evidences/results of certified product.

So far, we are focusing on a specific certification scheme/ standard (Common Criteria). As abovementioned existing collaboration networks exist in specific certification schemes.

The idea behind the perfect world vision would suggest to make the basis for improving the existing networks in cross-Certification Scheme direction.

As anticipated in section 4.1, evidences and results obtained in a certification could be useful and make faster a certification with a different certification schema probably because a set of evidences and assurance activities can be considered similar and probably re-used for making other certifications..

In this way, a complex network of Certification Bodies and “multi-certification scheme” laboratories could lead to perform more efficient and faster security certification.

Finally, another important aspect is related to the presence of Research Institutes as cybersecurity evaluation laboratories.

Research and certification could narrow the distance if the expertise of researchers is available for certification and not only. As described in section 5.2.1.2 complementary software tools used in certification process could benefit from R&D activities. This could be simpler if the network of evaluation laboratories will increment the cooperation with Research Institutes and R&D activities.

6.1 Laboratories network

Evaluation laboratories operate under respective national schemes (starting from Common Criteria certification). In this section we focus on the following nations:

- French scheme, operated by ANSSI: https://www.ssi.gouv.fr
- German scheme, operated by BSI: https://www.bsi.bund.de
- Italian scheme, operated by OCSI: www.ocsi.isticom.it
- Dutch scheme, operated by TÜV Rheinland NL and NLNCSA: http://www.tuvnederland.nl/
- Spanish scheme, operated by CCN: https://oc.ccn.cni.es/
- Swedish scheme, operated by FMV: http://fmv.se/
- Norwegian scheme, operated by SERTIT: http://www.sertit.no/

Even if they are providing services of evaluating the security of ICT products based on an approved and unified methodology, their legal and business context varies, reflecting characteristics of local economies and policies of the Certification Body. These laboratories can be

- Private company: independent legal entity, usually similar in form to a limited liability corporation,
- Traded private company: independent legal entity, traded on a local stock exchange,
- Research institute: non-profit entities, set up by industry members or universities, and
- Government agency: laboratories that are part of the country’s government.

Table 6 shown a list of nations with some information about their Certification Body and accredited laboratories. As abovementioned, the table shows the existence of a network between Certification Bodies and laboratories. In particular, by browsing Certification Bodies websites it is possible to access to existing international collaboration initiatives.

These collaboration activities are the foundation for the improvement and the creation of a more complex and structured collaboration.

Another important point is the accreditation of the laboratories at more Certification Bodies.

This point also leads to a more efficient network. It is likely that a laboratory accredited at more than one Certification Body can re-use and take advantage from experiences obtained during evaluation performed in different nations.

FRANCE	*The French Network and Information Security Agency (ANSSI) is responsible for examining certifications according to the directives given by the certification management committee.* *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.* *(Source www.ssi.gouv.fr)*	
	AMOSSYS	http://www.amossys.fr/
	CEA – LETI	http://www.leti.fr/en
	OPPIDA	http://www.oppida.fr/
	SERMA SAFETY & SECURITY	https://www.serma-safety-security.com/en/laboratories/itsef
	THALES/CNES	http://www.thalesgroup.com/
	Trusted Labs	http://www.trusted-labs.com/
GERMANY	*As a national cyber security authority, the goal of the Federal Office for Information Security (BSI) is to promote IT security in Germany. The BSI is first and foremost the central IT security service provider for the federal government in Germany. However, we also offer our services to IT manufacturers as well as private and commercial users and providers of information technology because effective security is only possible when everyone involved contributes. For this reason, we want to work in even closer co-operation with all those working in the IT and Internet industry in the field of IT security.* (Source http://www.bsi.bund.de/)	
	Atsec information security	http://www.atsec.com/
	Deutsche Telekom Security	http://geschaeftskunden.telekom.de/security
	Deutsches Forschungszentrum für künstliche Intelligenz (DFK)	http://www.dfki.de/
	Media transfer AG Prüfstelle für IT-Sicherheit	http://www.mtg.de/
	Secuvera	http://www.secuvera.de/
	SGS Digital Trust Services	http://www.sgs.com/cybersecurity-services
	SRC Security Research & Consulting	http://www.src-gmbh.de/
	TÜV Informationstechnik	http://www.tuvit.de/
ITALY	*OCSI manages the National Scheme for the evaluation and certification of the security of systems and products in the information technology sector; this National Scheme was established by the Prime Ministerial Decree of 30 October 2003 (G.U. n.98 of 27 April 2004).* *ISCOM (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione) of the Ministry of Economic Development is, by decree, the Certification Body for Information Security in the Information Technology sector. OCSI acts in accordance with the international ISO/IEC IS-15408 (Common Criteria) standards and the European ITSEC and ITSEM criteria* (Source www.ocsi.isticom.it)	
	Atsec information security	https://www.atsec.com/
	IMQ/LPS	http://www.imq.it/
	LVS - Selta	http://www.selta.com/

	LVS Leonardo (ex Consorzio RES)	http://www.leonardocompany.com/-/security-laboratorio-evaluation-valutazione-facility-sicurezza
	Technis Blu S.r.l.	http://www.technisblu.it/
	CCLab[4]	www.cclab.hu
NETHERLAND	*TÜV Rheinland Nederland B.V., as the Certification Body, certifies the security of IT products and systems in accordance with the procedures specified in the NSCIB scheme (Ref. [11]) documentation and the evaluation standards, criteria and methodology (Common Criteria Ref. [4]). TÜV Rheinland Nederland B.V. will take into account, amongst other evidences, the evaluation technical reports issued by the ITSEF, licensed as laid out in part 3 of the NSCIB scheme documentation.* (Source https://www.tuv-nederland.nl)	
	Brightsight BV	http://www.brightsight.com/
	Riscure BV	https://www.riscure.com/
	Secura B.V.	https://www.secura.com/
	UL TS	http://www.ul-ts.com
	TÜV Informationstechnik GmbH	http://www.tuvit.de
NORWAY	*Under the Norwegian Certification Scheme, impartial third-party assessment of IT security in products is performed in accordance with the internationally recognized standard Common Criteria (CC) or equivalent to ISO/IEC 15408. In its role as a certification body, SERTIT examines and approves the evaluation laboratory's reports, prepares a certification report and issues a certificate.* (Source http://www.sertit.no/)	
	Advanced Data Security	http://adseclab.com
	Norconsult ITSEF	http://www.norconsult.no/
	System Sikkerhet AS	https://systemsikkerhet.wordpress.com/
	Brightsight BV[5]	http://www.brightsight.com/
SPAIN	*In Spain, the evaluation and certification of an ICT security product responsibility is assigned to the National Cryptologic Centre (CCN) through Royal Decree 421/2004, 12th Marchin its Article 1 and Article 2.1, which establishes " setting up the Certifcation Body for the National Evaluation Scheme and Certification of Information Technology Security, to be applied to products and systems in its feld"* (Source https://oc.ccn.cni.es/)	
	Applus Laboratories	http://www.appluslaboratories.com/
	Centro de Evaluación de la Seguridad de las Tecnologías de la Información (CESTI), del Instituto Nacional de Técnica Aeroespacial (INTA)	http://www.inta.es/
	BRIGHTSIGHT BARCELONA S.L.	http://www.brightsight.com
	Clover Technologies	http://www.clovertechnologies.es/
	Dekra Testing and Certification	https://www.dekra.es/es/ciberseguridad-productos/

[4] As stated in https://ocsi.isticom.it/index.php/laboratori/lvs-accreditati CCLab accredited CSEF based in Hungary (accreditation is actually expired at 4 of April 2021)

[5] This CSEF is also accredited by Netherland Certification Body

	Layakk Seguridad Informatica (LSI)	http://www.layakk.com
	SGS Española de control	https://www.sgs.es/
SWEDISH	*CSEC - Swedish Certification Body for IT Security* *CSEC operates as Sweden`s national certification body for IT Security in products and systems according to the standard Common Criteria, CC. CSEC issues internationally recognised certificates.* (Source https://www.fmv.se/english/supplier-information/csec/)	
	atsec information security AB	https://www.atsec.com/
	Combitech AB	https://www.combitech.com/

Table 6: List of Certification Bodies and Evaluation Laboratories

Table 7 shows that evaluation laboratories have different typology. They can be part of a multi-national company or they can be part of government structure.

This heterogeneity can make more difficult to establish a “fluid” network for the information sharing because different companies can have different objectives and a different management of information sharing, at the same time also national economies and policies can impact on this interaction.

For this reason the definition and the agreement of a structured and well defined policy for sharing the information became fundamental in order to improve the network (e.g. establish which type of information can be shared, define a NDA at network level, etc.)

Country	Number of licenced labs	Private company	Trade Private company	Part of Multinational Corp	Research Institute	Government Agency
France	6	4	--	1	1	--
Germany	8	7	--	--	1	--
Italy	6	4	1	1	--	--
Netherlands	6	4	--	2	--	--
Norway	4	3	--	1	--	--
Spain	7	3	1	2	--	1
Sweden	2	2	--	--	--	--
Total	**39**	**27**	**2**	**7**	**2**	**1**

Table 7: Typology of Evaluation Laboratories

6.2 Collaboration between Certification Bodies

Table 8 shows, for each laboratory, which certification they can perform in adherence to the standards listed in columns.

A laboratory accredited for performing certification against more than one Certification standard can take advantage from the expertise of its own evaluators and evidences and results obtained in different certifications.

Let image a certification of the same product under different security certification standards using the same laboratory.

It is clear that the certification could be managed faster because some evidences, tools, procedures and assurance activities can be re-used across the different standards.

The perfect world vision aims to extend these principles by sharing information in a more structured and large way between different laboratories and in the same way between the Certification Bodies.

	CC	EMV CO[6]	FIPS[7]	GSMA	Mifare	PCI[8]
France						
AMOSSYS	X					
CEA-LETI	X	X			X	
OPPIDA	X					
SERMA	X	X	X	X	X	X
THALES/CNES	X	X				
Trusted Labs	X					
Germany						
Atsec	X		X[9]	X		
Deutsche Telekom Security	X					X
DFK	X					
Media transfer AG	X					
Secuvera	X					
SGS Digital Trust Services	X	X				
SRC	X	X				
TÜV IT	X	X	X			

[6] Source https://www.emvco.com/approved-registered/service-providers/?action=search_providers&px_search=&emvco_service_labs%5B%5D=acceptance-device&emvco_service_labs%5B%5D=card&emvco_service_labs%5B%5D=nfc-consumer-device&emvco_service_labs%5B%5D=security-evaluation

[7] Source https://csrc.nist.rip/groups/STM/testing_labs/

[8] Source https://www.pcisecuritystandards.org/assessors_and_solutions/pci_recognized_laboratories

[9] Accredited the USA company

	CC	EMV CO[6]	FIPS[7]	GSMA	Mifare	PCI[8]
Italy						
Atsec	X		X[9]	X		X
IMQ/LPS	X					
LVS - Selta	X					
LVS Leonardo	X					
Technis	X					
CCLab	X					
Netherland						
Brightsight BV	X	X		X	X	X
Riscure BV	X	X				
Secura B.V.	X					
UL TS	X					X
TUV IT	X					
Norway						
Advanced Data Security	X					
Brightsight BV	X			X	X	X
Norconsult	X					
System Sikkerhet A	X					
Spain						
Applus	X	X			X	
INTA	X					
Brightsight	X	X				
Clover	X					
Dekra	X			X		
LSI	X					

	CC	EMV CO[6]	FIPS[7]	GSMA	Mifare	PCI[8]
SGS	X					
Atsec	X		X	X		X
Combitech	X					

Table 8: CSEFs and certification standards

Chapter 7 Conclusions

The huge amount of different certification standards presented in this document brings to a consideration that want to share and optimize the different aspects of security.

It can be done in terms of experiences, skills of the different laboratories in the different nations considering also the sharing of evidences between different types of security certifications.

The improvement of the existing collaborations between certification bodies and accredited CSEFs, in the wide plethora of security certification standards presented in this document, could be an objective able to bring advantages in terms of time and costs of security certification.

Skills and tools, moreover, could benefit also by involving in certification process R&D and Research Institutes in a more structured way, in order to take advantage from competences of Subject Matter Experts and by using, for example, complementary software tools for performing vulnerability assessment and penetration test activities.

The vastness and the different typology of certifications presented in this document lead to a reflection that aims to bring together and optimize the different aspects of security in terms of experiences between different nations and laboratories, as well as in terms of sharing. evidences between different types of security certifications.

The creation of a worldwide “structured” network could bring to share better the evidences obtained during the certifications in the different standards.

This could be done thanks to the creation of a formally regulated, “cross-standard” network of collaboration between the laboratories, coordinated by a Steering Committee made up by the Certification Bodies.

The creation of a large, ordered and organized network would allow sharing the evidence obtained from the individual certifications of the various standards.

The idea is to take advance from re-using evidences, skills, tools and experiences on the one hand to optimize the overall security certification process and on the other end to make faster and cheaper the security certification.

From a worldwide vision, it probably will conduct to an improvement of overall security of the products available in the market. Faster and cheaper certification should motivate the company in investing on security certification (security certifications lead also to improve company reputation). This consequently will lead to increment the number of certified product available on the market.

The existence of this network could also benefit the certification "maintenance" activities that could be carried out more quickly by different laboratories based on evidence that is collected by the various certifications (just think about the possibility of maintaining the certificate for one standard and extending it to other standards).

For example:

- a product certified with a standard “X” for cryptographic algorithms updates its certification and obtains the maintenance of the certificate
- the same product certified against a security standard “Y” by re-using evidences of certification updated for security certification “X”, thanks to this network, could obtain a quickly maintenance of the certificate also on standard “Y”.

In order to do this, there are many issues to be addressed, along a roadmap that is certainly not short.

The first problem is that upon signing the contracts relating to a security evaluation, the related NDA is signed between the Developer / Sponsor and the CSEF. When formalizing an extended network of laboratories, the problem of extending the NDA to the entire network of laboratories should therefore be addressed.

It is therefore essential to establish what information can be shared between the various laboratories, what level of detail (e.g. exchange of configuration data instead of detailed design or development), where becomes necessary to be more rigid in "obliging" the exchange of information and where it is possible to be tolerant.

Finally, it will be important to address the issue about how exchange, store and process it in secure way. Probably the creation of the network could be not limited to a “high-level interaction network” but it should be extended to a “physical/logical network”. This will require establishing security requirements for implementing the necessary countermeasures in order to protect the information.

It is therefore necessary to work on a shared path between the various stakeholders described in this document that allows the creation and formalization of this network:

- rationalizing the skills and tools adopted by different CSEFs for different standards
- formally establishing a network of laboratories coordinated by a steering committee of Certification bodies
- establishing the type of information that can be shared within this network (starting from evaluating how the information subject to NDA can be managed and disseminated within this network)
- establishing security requirements for protecting the transmission, processing and storage of information inside the supporting “physical/logical network” of CSEFs and Certification Bodies.

Chapter 8 List of Abbreviations

Abbreviation	Translation
3GPP	3rd Generation Partnership Project
AB	Accreditation Body
ADV	Assurance class Development
AEI	Agrupación Empresarial Innovadora
AGD	Assurance class Guidance Documents
ALC	Assurance class Life-Cycle
ANSSI	Agence nationale de la sécurité des systèmes d'information
API	American Petroleum Institute
AR	Activity Reports
ASE	Assurance class Security Target
ATE	Assurance class Test
AVA	Assurance class Vulnerability Assessment
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI	British Standards Institution
BSIMM	Building Security in Maturity Model
BSPA	Baseline Security Product Assessment
CAPE	Continuous assessment in polymorphous environments
CAPS	CESG Assisted Products Scheme
CAB	Conformity Assessment Bodies
CB	Certification Body
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CIP	Critical Infrastructures Protection
CIS	Center for Internet Security
CLEF	Commercial Licensed Evaluation Facilities

Abbreviation	Translation
CPA	Commercial Product Assurance
CREST	Council for Registered Ethical Security Testers
CS	Cyber Security
CSA	Cloud Security Alliance
CSEF	Cyber Security Evaluation Facilities
CSIRT	Cyber-Security Incident Response Team
CSPN	Certification de Sécurité de Premier Niveau des Produits des Technologies de l'Information
DHS	Department of Homeland Security
DSP	Digital Service Providers
DPCM	Decreto del Presidente del Consiglio dei Ministri
EBA	European Banking Authority
EAL	Evaluation Assurance Level
EC	European Commission
ECSO	European Cyber Security Organization
EMVCo	Europay, Mastercard, and Visa Consortium
ENISA	European Network and Information Security Agency
ENS	Esquema Nacional de Seguridad
EP	Evaluation Plan
ETR	Evaluation Technical Report
EU	European Union
EUCC	Common Criteria based European cybersecurity certification scheme
EuroPriSe	European Privacy Seal
FINCSC	Finnish Cyber Security Certificate
FIPS	Federal Information Processing Standards
HSM	Hardware Security Model
ICCC	International Conference on Computer and Communications

Abbreviation	Translation
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISCOM	Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione
ITSEC	Information Technology Security evaluation criteria
ISO	International Standards Organization
MRA	Mutual Recognition Arrangement
NCA	National Competent Authorities
NDA	Non-Disclosure Agreement
NITES	National IT Evaluation Scheme
NSA	National Security Agency
OES	Operators of Essential Services
OR	Observation Report
OT	Operational Technology
PP	Protection Profile
PT	Penetration Test
SIG	Software Improvement Group
SME	Subject Matter Expert
SOG-IS	Senior Official Group – Information System Security
TOE	Target of Evaluation

Chapter 9 Bibliography

[1] James Anderson, Computer Security Technology Planning Study, ESD-TR-73-51, U.S. Air Force Electronic Systems Division (1973).

[2] Department of Defense, “Department of Defense Trusted Computer System Evaluation Criteria,” DoD 5200.28-STD (Dec 1985).

[3] Office for Official Publications of the European Communities, Information Technology Security Evaluation Criteria (ITSEC) Provisional Harmonised Criteria, June 1991, Document COM(90) 314

[4] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model, CCMB-2017-04-001, Part 2: Security functional components CCMB-2017-04-002 and Part 3: Security assurance components, April 2017 Version 3.1 Revision 5

[5] Ross Anderson, Mike Bond, Jolyon Clulow and Sergei Skorobogatov, “Cryptographic processors - a survey”, Cambridge University Computer Laboratory Technical Report no. 641 (July 2005)

[6] National Voluntary Laboratory Accreditation Program (NVLAP), “Procedures and General requirements”, NIST Handbook 150, 2020 edition

[7] Melissa Azouaoui, Davide Bellizia, Ileana Buhan, Nicolas Debande, Sébastien Duval, Christophe Giraud, Eliane Jaulmes, François Koeune, Elisabeth Oswald, François-Xavier Standaert and Carolyn Whitnall, « A systematic appraisal of Side Channel Evaluation Strategies »,

[8] SPARTA CAPE D5.1 Assessment specifications and roadmap, , 31st January, 2020 https://www.sparta.eu/assets/deliverables/SPARTA-D5.1-Assessment-specifications-and-roadmap-PU-M12.pdf.

[9] SPARTA CAPE D5.2 Appendix B Protection Profile for a Safety and Security Platooning Management Module, 29th January 2021.

[10] ENISA, “EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS” V1.0 | 01/07/2020, https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme

[11] TÜV Rheinland Nederland B.V. , Netherlands Scheme for Certification in the Area of IT Security (NSCIB), document version 2.5, 28 March 20190

[12] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," in IEEE Security & Privacy, vol. 9, no. 3, pp. 49-51, May-June 2011, doi: 10.1109/MSP.2011.67.

[13] ISA (International Society of Automation) Blog, “Lessons Learned from a Forensic Analysis of the Ukrainian Power Grid Cyberattack https://blog.isa.org/lessons-learned-forensic-analysis-ukrainian-power-grid-cyberattack-malware

[14] Baezner, Marie & Robin, Patrice. (2018). Cyber and Information warfare in the Ukrainian conflict.Risk Based Security, “Cyber Risk Analytics 2019 MidYear QuickView Data Breach Report”, August 2019, https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

[15] Verizon, “Data Breach Investigations Report 2020,” https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf

[16] Independently conducted by Ponemon Institute LLC and jointly developed by Accenture, “The cost of Cybercrime ninth annual cost of cybercrime study unlocking the value of improved cybersecurity protection”, 2019, https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

[17] Conducted by Ponemon Institute and sponsored by IBM Security, “Cost of a Data Breach Report 2019”, https://www.ibm.com/downloads/cas/RDEQK07R#:~:text=The%20time%20between%20when%20a,a%20total%20of%20279%20days.

[18] 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”

[19] A. Morgagni, P. Massonet, S. Dupont and J. Grandclaudon, "Towards Incremental Safety and Security Requirements Co-Certification," 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2020, pp. 79-84, doi: 10.1109/EuroSPW51379.2020.00020.