Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D7.7

The Role of Certification and its Implementations

Document Identification	
Due date	30 June 2022
Submission date	30 June 2022
Revision	3.0

Related WP	WP7	Dissemination Level	PU
Lead Participant	CYBER	Lead Author	Liina Kamm (CYBER)
Contributing Beneficiaries	UMU, BRNO, CONCEPT, ARCH, UPS-IRIT	Related Deliverables	3.22, 7.4, 7.5, 8.4

Abstract: This deliverable describes the challenges of certification, different certification schemes, testing approaches and risk assessment approaches. We describe and validate a virtual certification centre, and validate the certification framework proposed in D3.22 Validation and Certification Methodology. We also take a look at the role of cyber security certification and its implementations for different organisations in Europe.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

The verification of declared characteristics of a product, process, person or organisation is known as certification. This deliverable aims to understand and document the role of cybersecurity certification and its implementations for devices and systems for the EU industry and provide solutions for the shortcomings. We discuss the challenges of cybersecurity certification.

To see the extent of the involvement of EU organisations in cyber security certification, we sent out a questionnaire to project partners and affiliated entities to find out about their involvement with certification whether as a provider of certification services or an owner of certified products, processes or people. The results have been summarised in Annex A of this document. Based on these results, we identified the most utilised methods. We give an overview of the state of the art of certification schemes, testing approaches and risk assessment approaches.

We envision and implement a virtual certification centre on top of the seccerts tool developed in the work package. We validate the virtual certification centre and the SURFACE certification framework (proposed in D3.22 Validation and Certification Methodology) using and integrated circuit (namely, the Estonian ID card chip) as a case study.

Document information

Contributors

Name	Partner
Liina Kamm	CYBER
Dan Bogdanov	CYBER
Jayavarshini Thirumalai	CYBER
Sara Nieves Matheu García	UMU
Pasquale Annicchino	ARCH
Mark Miller	CONCEPT
Victoria Menezes Miller	CONCEPT
Petr Svenda	BRNO
Katia Jaffrès-Runser	UPS-IRIT
Peter Hamm	GUF

Reviewers

Name	Partner
Vaclav Matyas	BRNO (high level review)
Jozef Vyskoc	VaF

History

Version	Date	Authors	Comment
0.01	2020-01-09	Liina Kamm, Sara Nieves Matheu García	Initial document structure
0.02	2020-01-21	Sara Nieves Matheu García, Pasquale Annicchino, Dan Bogdanov, Liina Kamm	Initial document content
0.03	2020-03-10	Liina Kamm, Mark Miller, Victoria Menezes Miller, Katia Jaffrès-Runser,	Contributions to second draft. Questionnaire results analysed

		Pasquale Annicchino, Sara Nieves Matheu García, Petr Svenda	
0.04	2020-03-18	Liina Kamm, Sara Nieves Matheu García, Petr Svenda, Pasquale Annicchino	Comments and contributions to the third draft taken into account. Introduction, executive summary.
0.05	2020-03-27	Liina Kamm, Dan Bogdanov	Some reviewer comments incorporated
1.0	2020-03-31	Liina Kamm, Sara Nieves Matheu García	Added final modifications based on reviewer comments. Added future work section.
1.1	2021-02-17	Liina Kamm	Initial document for second internal version
1.2	2021-04-15	Liina Kamm, Sara Nieves Matheu García, Pasquale Annicchino, Katia Jaffrès-Runser, Petr Svenda, Jayavarshini Thirumalai	Consolidated input for the second internal version
1.3	2021-04-27	Liina Kamm, Katia Jaffrès-Runser, Mark Miller	Draft version for internal review
2.0	2021-05-31	Liina Kamm, Sara Nieves Matheu García	Added final modifications based on reviewer comments.
2.1	2021-12-12	Sara Nieves Matheu García, Petr Svenda	Virtual Certification Centre concept
2.2	2022-02-01	Liina Kamm	Added validation of the certification methodology
2.3	2022-05-05	Sara Nieves Matheu García, Petr Svenda, Liina Kamm	Virtual Certification Centre main text
2.4	2022-05-15	Liina Kamm, Sara Nieves Matheu García, Petr Svenda	Document for high level review
2.5	2022-06-13	Liina Kamm	Incorporated WPL comments. Document for review
2.6	2022-06-20	Peter Hamm	Minor formatting updates
2.7	2022-06-28	Liina Kamm, Sara Nieves Matheu García, Petr Svenda	Reviewer comments incorporated
3.0	2022-06-29	Liina Kamm	Final version for submission
3.0	22-06-30	Ahad Niknia	Final check, preparation and submission

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**ANSI**	American National Standards Institute
	ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
C	**CC**	Common Criteria
	CCRA	Common Criteria Recognition Arrangement
	CERT	Computer emergency response team
	CESG	Communications-Electronics Security Group
	CM	Continuous monitoring
	CNSSI	Committee on National Security Systems Instruction
	CPA	Commercial product assurance
	CPS	Cyber-physical systems
	cPP	Collaborative Protection Profiles
	CSPN	Certification de Sécurité de Premier Niveau
	CVE	Common vulnerabilities and exposures
	CVSS	Common vulnerability scoring system
	CWSS	Common weakness scoring system
D	**DSL**	Domain specific language
	DGC	Dependency-guarantee relationship
	DGR	dependency-guarantee contract
E	**EAL**	Evaluation assurance level
	ECSO	European Cyber Security Organization
	EG	Expert group
	ENISA	European Union Agency for Cybersecurity

	ETR	Evaluation technical report
	EUCC	European Candidate Cybersecurity Certification Scheme
F	**FAIR**	Factor analysis of information risk
	FOSS	Free and open-source software
G	**GDPR**	General Data Protection Regulation
	GPP	Generalized Protection Profile
H	**HARM**	Hailstorm Application Risk Metric
I	**IEC**	International Electrotechnical Commission
	ISCM	Information Security Continuous Monitoring
	ISO	International Organization for Standardization
M	**MBT**	Model-based testing
	MBST	Model-based security testing
	MIA	Model inference assisted
	MRA	Mutual recognition agreement
N	**NIST**	National Institute of Standards and Technology
	NVD	National vulnerability database
O	**OCL**	Object constraint language
	OCTAVE	Operationally critical threat, asset, and vulnerability evaluation

	OSSTMM	Open source security testing methodology manual
	OWASP	Open Web Application Security
R	**ROE**	Rules of engagement
	RTU	Remote terminal units
S	**SA**	Safety argument
	SAST	Static application security testing
	SC	Safety case
	SCA	Static code analysis
	SEI	Software Engineering Institute
	SUT	System under test
T	**TOE**	Target of evaluation
U	**UL**	Underwriters Laboratories
	UL CAP	Underwriters Laboratories Cybersecurity Assurance Program

1 Introduction

Certification is the confirmation of specific characteristics of a product, process, person or organisation. In most cases, assurance is obtained through an independent qualified external review, evaluation or audit. An accredited third party assesses the characteristics, quality and qualifications of the object or person. This assessment is carried out in accordance with established requirements or standards. As this is a very wide and diverse area, we will focus on the certification of products (devices and systems) in this deliverable.

Mission critical services of an information society, including but not limited to strong authentication, digital signature creation and encryption, must be certified before deployment in a pan-European setting. There are already well-functioning precedents, such as the eIDAS regulation that sets clear requirements for digital signature devices and the medical devices regulation/in-vitro diagnostics regulation (MDR/IVDR) that dictate requirements for medical devices. A similar approach could solve the challenges in cybersecurity certification, if designed with an approachable level of complexity.

1.1 Goals of Cybersecurity Certification

Certification, at a general level, supports the adoption of complex technologies, products and services, or helps accredit the skillsets of a person. It also contributes to the increase of trust among end-users. By agreeing on a set of requirements, customers can start demanding a product from vendors that satisfies these requirements. Given that validating the claims of a vendor requires a comparable level of technological skills, it is infeasible for most customers to do it by themselves. Instead, they trust that a certification body has worked with the vendor to ensure that the product satisfies the joint requirements. The certification body in turn has been accredited by an accreditation body that has its own set of standards and rules for assessing the trustworthiness of a certification body.

Cybersecurity is a subdomain of information technology and, thus, inherits its rapid speed of development. New products and technologies address challenges faced by governments and industry, including, but not limited to satisfying data protection (e.g., anonymisation) requirements for new services, authenticating parties in ever-growing networks (web, IoT), resolving identities against federated sources of trust, detecting anomalies in networks and logs, ensuring a safe behaviour of the embedded software and networks, and ensuring the integrity of the software and data.

However, in the early stages of development, technologies responding to these demands can only be deployed by parties with technical teams capable of supporting the integration work. This, in turn, could hinder the adoption of technologies needed to secure the European Digital Single Market and global digital markets.

To find out the current status of certification in Europe, we conducted a survey among the project partners, affiliated entities and other parties in Europe. Based on the answers we identified the most used certification schemes, testing and risk assessment methods. We then put together an overview of these schemes and methods and identified the challenges that are inherent in the system.

1.2 Barriers to Adoption

There are different challenges in certification: the heterogeneity of certification schemes, the prohibitive cost and long process, the difficulty of recertification within the product lifecycle, the composition of certification within a larger product, the comparability of certification levels. These challenges often discourage manufacturers and vendors from certifying products unless required to do so by law.

To deal with these issues, we have developed a support framework for certification (SURFACE, Deliverable 3.22 *Validation and Certification Methodology*) and in this deliverable we propose a virtual certification centre built on top of the seccerts tool developed in Work Package 7 (*Open Tools and Infrastructures for Certification and Validation*). The centre by itself focusses on dealing with the

structuring and availability of certification results but if used together with SURFACE, they create an ecosystem that mitigates the most pressing issues and gives a strong foundation to bringing certification closer to the manufacturers and vendors as well as the end-users by simplifying the process of deciding what the certificates actually mean and which certificates give an adequate level of assurance for their purposes. In this deliverable, we describe the certification centre and give an example based validation of both the support framework and centre.

1.3 Document Structure

We begin, in Section 2, by giving an overview of the most common certification schemes used in cybersecurity. Section 3 talks about testing approaches and Section 4 considers risk assessment approaches. In Section 5, we discuss the different challenges of certification and, in Section 6, we talk about the role of the European Cybersecurity Act in certification and how this will affect the challenges. Section 7 describes the virtual certification centre. Section 8 uses an example-based validation for the virtual certification centre and an application of the SURFACE framework presented in Deliverable 3.22 *Validation and Certification Methodology*. Appendix A summarises the certification questionnaire (given in Appendix B) results that were obtained from project partners and associated entities.

2 Cybersecurity Certification Schemes

This section analyses the main cybersecurity certification schemes for software and hardware. We also bring out their shortcomings, which will further be discussed in Section 5. In order to analyse developments at the EU level one must look at the EU cybersecurity certification framework for ICT digital products, services and processes as established by the EU Cybersecurity Act. The EUCC proposed by ENISA following the request of the European Commission. The GDPR certification schemes have been studied recently in a report published by the European Commission that we can use as a main source[1]. There also exists an ECSO report on the different schemes[2].

2.1 Common Criteria

The most well-known cybersecurity certification standard is the Common Criteria (CC) [1], in which the functional and assurance requirements for security are specified as a list from a catalogue or through protection profiles (PPs) for a target of evaluation (TOE), which is a set of software, firmware and/or hardware. These requirements are defined in the security target (ST) description. Initially, vendors were specifying TOE themselves, together with corresponding functional and assurance requirements as needed for the target security level. As of roughly 2010, it became popular to use Protection Profiles as the templates for certifying an item. A particular PP specifies the requirements relevant for the particular domain, e.g., network firewall or cryptographic service provider.

CC permits comparability between the results of independent cybersecurity evaluations providing a common set of requirements for the security functionality of IT products. This is obtained through collaborative protection profiles (cPPs), which become available for use under the terms of the Common Criteria Recognition Arrangement (CCRA) [2]. Evaluations conducted against cPPs are mutually recognised according to the terms of the CCRA. The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to them meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfil their security needs. For this purpose, it uses Evaluation Assurance Levels (EALs) to describe numerically the depth and rigor of an evaluation. Basically, CC assurance is achieved by carrying out analyses and checking processes and procedures, guidance documents, TOE design, functional tests, independent functional testing, vulnerabilities and penetration testing [3].

Although CC is the main standard, the community has identified several limitations [4], [5] that are being considered. Examples of them are the time and effort required to

- document the product itself (i.e., its design, development, testing, distribution, deployment, removal) and its evaluation process,
- gather evidence, in particular at higher EALs,
- manage the changes in the certified product.

During the manufacturing process, this could involve market delays and, therefore, result in considerable financial loss. It is worth noting that CC evaluation is focused on a specific version of the TOE, including the configurations. This means that any change over in the TOE (e.g., a new vulnerability) could invalidate the result of the certification, something that is quite critical in frequently updated products. In addition, recertification is not mandatory in CC, and the responsibility of informing about security changes lies with the owner of the certificate. As a result, the certification category with the largest

[1] https://ec.europa.eu/info/sites/info/files/data_protection_certification_mechanisms_study_final.pdf
[2] https://ecs-org.eu/documents/publications/5a31129ea8e97.pdf

number of active certificates is ICs, smart cards and smart card-related devices and systems, where certified items tend to be long-lived with relatively few updates (if any)[3].

2.2 Commercial Product Assurance

The Commercial Product Assurance (CPA) [6] is the UK national scheme from the Communications-Electronics Security Group (CESG) in charge of assessing the security level of a TOE, testing and certifying both software and hardware within the UK government [7]. CPA security characteristics against which the products are assessed are published in [6].

If a product passes the CPA assessment, it is awarded with the Foundation Grade certificate, valid for two years and allowing any type of update required, leading in some way with the dynamicity of the security changes [6]. However, recertification will only happen if a security change is known within an update and the manufacturer wishes to update it. This takes about 6 months [7].

The main barrier of CPA is that there is no Mutual Recognition Agreement (MRA) for it, meaning that if a product was certified in the UK it will not usually be accepted outside. However, this is being addressed through the so-called CPA mapping for the Protection Profile that was used in the CC evaluation of the product. This evaluation performs a mapping between the protection profile of CC and the security statements of CPA.

2.3 Cybersecurity Assurance Program

Underwriters Laboratories (UL) is a company that certifies that electrical, building, fire, mechanical and other products follow the UL standards. The company created its Cybersecurity Assurance Program (UL CAP) in 2016. The program uses the UL 2900 standards [8]. This series of standards aims to provide a series of technical criteria to evaluate the security of a TOE.

However, these standards were created by a for-profit enterprise and they were not published so that the research community could validate them. This has raised a lot of criticism. Due to its recent creation, it is not widely recognized as an accepted certification scheme. The standard has three parts:

1. Outline of Investigation for Software Cybersecurity for Network-Connectable Products, General Requirements (UL 2900-1),
2. Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Particular Requirements for Network Connectable Components of Healthcare Systems (UL 2900-2-1), and
3. Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Particular Requirements for Industrial Control Systems (UL2900-2-2).

The latter applies to the evaluation of industrial control systems components, such as process control systems, control servers, SCADA servers, remote terminal units (RTU) or smart sensors, among others. However, only the first part has been published as an American National Standards Institute (ANSI) standard.

Regarding recertification, in case there is a major change, the product must be certificated completely. There is no lightweight alternative process.

2.4 European Cybersecurity Candidate Scheme

The goal of the European Network and Information Security Agency (ENISA) is to guide on generating common standards or policies across the EU. The European Cybersecurity Candidate (EUCC) scheme [9] from ENISA provides a set of guidelines, rules and regulations based on Common Criteria for

[3] Common Criteria portal, Certified Products List – Statistics. https://www.commoncriteriaportal.org/products/stats/. April 2021

evaluating an ICT product. These guidelines are in compliance with the requirements of the Cybersecurity Act [10]. By following these guidelines, we can define a standardised framework that supports multiple ICT products. The major benefits of implementing standardised criteria and methods for cybersecurity evaluation are, for example, consistency between different manufacturers and vendors, re-usability, harmonisation of terminology, awareness [10].

2.5 Certification de Sécurité de Premier Niveau

The Certification de Sécurité de Premier Niveau (CSPN) [11] is a French standard created by the National Cybersecurity Agency of France (ANSSI) in 2008. CSPN ensures independence through the auditors, who have to be accredited by ANSSI. The objective of this scheme is to verify the compliance of the product in relation to its specifications, assessing against the known vulnerabilities and stressing the product with tests aiming to break its security. The evaluation includes conformity analysis (verifying that the product complies with its security specifications) and efficiency analysis (measuring the strength of the security functions and mechanisms). One of the key points of CSPN is that the evaluation is performed in a short period of time through the adaptation of the product development lifecycle, reconciling time needs of the manufacturing with the security assessment.

The CSPN approach starts by defining the security target (ST), describing the scope of the evaluation. After that, the ST is validated by ANSSI and all the needed material is gathered by the evaluator (e.g., source code, a functional version of the product, historical data, and documentation). Then, the product is evaluated, allowing exchanges between the evaluator and the developers by providing extra material or giving information. This step includes the redaction of a detailed report that should include the test considered during the certification process, their results and the uncovered issues. After the evaluation, ANSSI validates the conclusions of the report. The final step is the delivery of the CSPN certificate by ANSSI in case of successful outcome of all the previous steps [12].

CSPN is complementary to CC, as it can be used to perform a short security evaluation to reduce the effects of an inadequate consideration of the security issues, and to prepare the TOE for the CC evaluation. Studies have shown that it is possible to reduce the CC costs by 10% [13]. Therefore, CSPN can be considered as a more lightweight certification methodology than CC, in which a certain product or system is evaluated within a short period of time (a typical certification can take between 35 days and 2 months) with a reduced cost (about 25.000-35.000 Euros). However, it is standard only in France, there is not a MRA related to it, so it does not foster a harmonized cybersecurity certification approach. Moreover, the concept of labelling is not considered, and it requires a complete certification process in case of any change on the security level of a certain product.

2.6 Certification in Avionics

Avionics is a field where certification is taken very seriously. When a serious vulnerability is found, it could result in actual casualties not only significant monetary and reputation loss. We look at avionics as an example of what a field with compulsory certification deals with.

Commercial airplanes and general aviation are regulated to ensure the safe transport of citizens. In the EU, the European Union Aviation Safety Agency[4] (EASA) is in charge of determining the rules for airworthiness and environmental certification. These rules are defined in certification specifications (CS), e.g., CS-25 details the rules for large aeroplanes, CS-E for engines.

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

2.6.1 Airworthiness Directives

Airworthiness directives (AD) are issued by EASA, acting in accordance with the basic regulation on behalf of the European community, its member states and of the European third countries that participate in the activities of EASA under Article 66 of that Regulation. ADs applicable to an EASA approved type certificate are those ADs which have been issued or adopted by the agency. ADs are issued by the agency through agency decisions.

The EASA Safety Publications Tool[5] offers a complete list of airworthiness directives that have been issued or approved by EASA since 28/09/2003. The tool also contains all proposed airworthiness directives (PAD) and allows users to submit their comments during the consultation period.

2.6.2 Aircraft Certification

Before a newly developed aircraft model may enter into operation, it must obtain a type certificate from the responsible aviation regulatory authority. Since 2003, EASA is responsible for the certification of aircrafts in the EU and for some European non-EU Countries. This certificate testifies that the type of aircraft meets the safety requirements set by the European Union.

The 4 steps of the type-certification process are the following.

1. **Technical familiarisation and certification basis.** The aircraft manufacturer presents the project to EASA when it is considered to have reached a sufficient degree of maturity. The EASA certification team and the set of rules that will apply for the certification of this specific aircraft type are being established (certification basis).
2. **Establishment of the certification programme.** EASA and the manufacturer need to define and agree on the means to demonstrate compliance of the aircraft type with each requirement of the Certification Basis. This goes hand in hand with the identification of the "level of involvement" of EASA during the certification process.
3. **Compliance demonstration.** The aircraft manufacturer must demonstrate compliance of its product with regulatory requirements: the structure, engines, control systems, electrical systems and flight performance are analysed against the certification basis. This compliance demonstration is done by analysis during ground testing (such as tests on the structure to withstand bird strikes, fatigue tests and tests in simulators) but also by means of tests during flight. EASA experts perform a detailed examination of this compliance demonstration, by means of document reviews in their offices in Cologne and by attending some of these compliance demonstrations (test witnessing).
   This is the longest phase of the type-certification process. In the case of large aircraft, the period to complete the compliance demonstration is set at five years and may be extended, if necessary.
4. **Technical closure and issue of approval.** If technically satisfied with the compliance demonstration by the manufacturer, EASA closes the investigation and issues the certificate. EASA delivers the primary certification for European aircraft models which are also being validated in parallel by foreign authorities for operation in their airspaces, e.g., the FAA for the US or TCCA for Canada. Conversely, EASA will validate the FAA certification of US aircraft models (or TCCA certification of Canadian models) according to applicable bilateral aviation safety agreements between the EU and the concerned third country.

[5] http://ad.easa.europa.eu/

2.6.3 Cybersecurity in Aviation

EASA has developed a cybersecurity roadmap. EASA is working on its implementation and a number of initiatives have been launched to better address cybersecurity risks in aviation improving resilience and fostering built-in security. In the summer of 2019, eligible organisations have been invited to join the cybersecurity group European Centre of Cybersecurity in Aviation (ECCSA).

The achievement of a cyber resilient aviation system and the incorporation of cybersecurity into the current safety notion require a coordinated effort of the aviation system stakeholders.

To this extent EASA participates and chairs the European strategic coordination platform that includes representatives of key industry stakeholders, member states and EU institutions. The collaboration is contributing to harmonise the objectives of aviation stakeholders and has made possible the development of the first common strategy for cybersecurity in aviation[6], in accordance with aspirations and principles stated in the agreed charter. The involved stakeholders are also in the process of defining a common roadmap in order to implement this strategy.

2.7 Towards Certified-by-Design IoT-Enabled Cyber-Physical Systems

Cyber-physical systems (CPS) may leverage IoT devices to acquire the physical state information using sensors and steer the system by sending commands to actuators. Vehicles such as autonomous cars, airplanes, satellites or drones leverage (in part sometimes) the CPS paradigm to improve the safety level of its use cases. Safety is ensured through various aspects, such as robustness, real-timeliness or security. The one we consider is real-timeliness: the capacity of a system to react in a bounded time to a drastic change measured in the environment, or to a command issued by its user.

These critical systems are steered using wired embedded networks that interconnect computing units that generally leverage a virtualised environment. Virtualisation ensures that applications run in their own isolated environment. Examples of such virtualised distributed frameworks are Integrated Modular Avionics (IMA) [14] for aircrafts or Autosar[7] for cars. The APEX [15] standardises the avionics application interface that is offered by the virtualised environment in IMA. It defines for each computing unit a fixed schedule that allocations fixed portions of time to the avionics applications. The schedule is called the Major time Frame (MAF). This MAF is designed offline. At runtime, it repeats indefinitely to offer processing time to application. The embedded networks interconnecting these computing units offer real-time guarantees: for any message emitted on the network, it is possible to calculate a bound on the worst-case communication delay between the transmitter and the receiver [16] [17].

To ensure safety by avoiding a single point of failure, IMA enforces a completely distributed setting. Thus, computing units are not synchronized, leading to a more complex determination of the real-time behaviour of the complete systems if hard real-time applications exchange critical information as shown in [18]. It is possible to design optimal temporal allocation of MAFs in a distributed avionics system as shown in [19]. This design ensures timeliness of all communications and all applications. Using multicriteria optimisation, it favours the choice of allocations that balance computing load with communication delay margins.

The design of safe cyber-physical systems that rely on wireless instead of wired systems is still an open issue. Our work in the CyberSec4Europe project aims at tackling the problem of designing a CPS using IoTs that are interconnected with a real-time wireless communication protocol. Here, sensors and

[6]https://www.easa.europa.eu/sites/default/files/dfu/Cybersecurity%20Strategy%20-%20First%20Issue%20-%2010%20September%202019.pdf

[7] Autosar consortium web page. January 2014. http://www.autosar.org.

actuators are operated by small edge computing platforms (ARM/Cortex microcontrollers or small computers such as Raspberry PI). These computing platforms have to leverage a real-time operating system (such as FreeRTOS, Keil RTX, RIOT) that schedules IoT applications related to measuring or steering the distributed CPS. For the full CPS to be real-time, the wireless communication protocol stack has to offer real-time guarantees knowing the data flow characteristics that are exchanged by applications. Typical wireless technologies such as IEEE802.15.4e (TSCH) can be leveraged to do so [20].

As we know beforehand that we want the system to be certified, we can already take certification into account during the design phase of the CPS. Later, the designs can be used to automatically conduct testing for certification. However, first the certified-by-design IoT-enabled CPS design problem has to be formulated. Knowing the IoT task description (worst-case computing duration, maximum activation period, input/output of sensor and actuator data, relative computing deadline) and network resource availabilities (TSCH resources blocks), the framework will design the schedule of IoT tasks on each edge node and the wireless communication schedule that guarantees that:

- the computing load of edge nodes are reduced,
- all computing deadlines of IoT tasks are met,
- end-to-end computing delays are below their deadline.

Second, this ongoing work will leverage mathematical models of system edge load and worst-case communication delay calculation to select the CPS instances that offer the best trade-off between an even network resource provision and edge node resource provision.

Third, the proposed framework will be rolled out on real devices (OpenMote B with Contiki NG embedded operating system). Design performance will be measured in terms of task computing times and message communication delays, and compared to the worst-case delay requirements.

2.8 Virtual Certification Centre: the ARMOUR Example

The ARMOUR[8] project was aimed at providing duly tested, benchmarked and certified security and trust technological solutions for large-scale IoT using upgraded FIRE large-scale IoT/cloud testbeds properly-equipped for security and trust experimentations. This project developed a security evaluation methodology combining risk assessment and testing based on ETSI and ISO standards. This methodology has been used as the baseline for the development of the certification methodology proposed in Deliverable 3.8 – Framework and Toolset for Conformity and developed further in Deliverable 3.22 - Validation and Certification Methodology.

As part of the work performed in ARMOUR, they defined a virtual certification centre intended to provide online certification related services such as the development of security profiles for a product or customer, risk assessment and test plan, risk analysis for non-expert vendors, security testing based on a test plan, services for monitoring on and after deployment and generation of the security label. Furthermore, accredited test services when available could be offered such as security tests for oneM2M under oneM2M accreditation, for Lora or ITS. All these services were offered by some of the ARMOUR partners (ODINS, EGM and SYN).

As one partner cannot provide the full list of services or a testing plan in particular field while other partner might have the requested expertise ARMOUR also defined a possible virtual certification with one contact for one-stop services. The European virtual certification centre would act as a European contact for all services on IoT security and certification, providing a common place for ensuring maintenance and information exchange for IoT certification and new threats. In this way, documents, useful information and services with their test plan could be located in single place.

[8] https://cordis.europa.eu/project/id/688237

This virtual centre was intended to be located in www.iot-certification.eu. However, the virtual centre was not implemented in reality and ARMOUR only provided a detailed description[9] of how the virtual centre was meant to be, as shown in Figure 1.

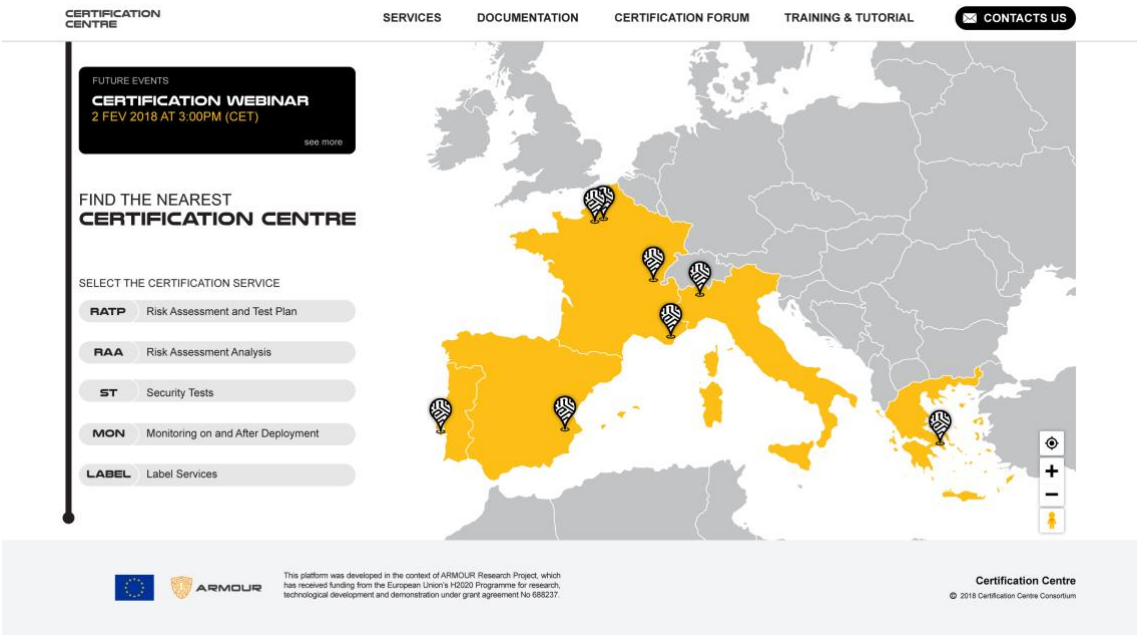

Figure 1: ARMOUR virtual certification centre, main page

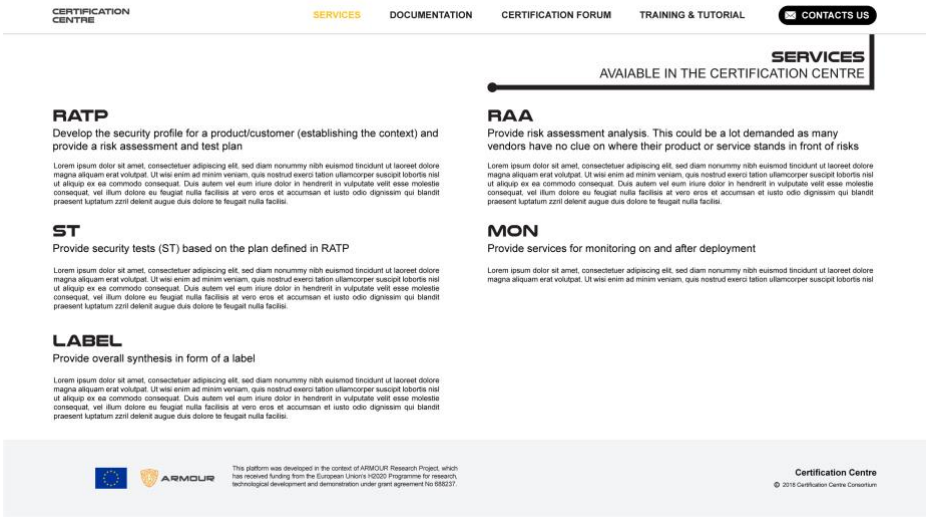

Figure 2 ARMOUR virtual certification centre, services page

The main webpage (Figure 1) can locate all the entities in the certification centre that can provide some certification services, and the services provided are identified in the list on the left side of the page. When one selects a service, a short description of the service is presented and only the entities that

[9] D4.5 ARMOUR project. Internal document

provide that service are shown. The Services page (Figure 2) describes all the certification services provided by the certification portal, providing the visitor with a detailed overview of services provided. The Documentation page shows resources to support the certification activities (e.g., Security Vulnerabilities and Test Patterns identified in ARMOUR). The web also includes a forum that can be used to communicate with experts to ask for guidance on a specific point and to discuss different views on some resources or procedures. Finally, the Training and Tutorials page lists the upcoming training events, like webinars, and the past events. In another section of the page are presented guides and tutorials that the visitor can read to learn more about a specific topic of the certification process.

3 Testing Approaches

This Section reviews the main security testing approaches that can serve as a tool for cybersecurity certification. Following the definition of CNSSI-4009 [21], security testing is the process of determining that an information system protects data and maintains functionality as intended. We call the system that being tested a system under test (SUT), which can be an information system consisting of specific business logic, but also a product or device that may be certified separately. A system under test (SUT) is a target of evaluation (TOE) but a TOE does not necessarily need to be a SUT.

Testing provides an empirical and objective way to verify if a vulnerability is present or not in the SUT or if the SUT is compliant with a certain requirement. Supporting certification with testing and evaluation assurance levels (EALs) to determine the depth of the testing procedure, allows a more objective and homogeneous evaluation. Moreover, the large amount of IoT system models to be certified requires the design of cost-effective testing procedures. Ideally, these techniques should be applicable to different types of systems and devices, in such a way that similar procedures could serve to certify the security level of different components. Security certification also has to deal with continuous security changes, due to new vulnerabilities or even updates and patches. Therefore, the security testing methodology should be able to manage the frequent changes associated to the security level of a product and integrated throughout the lifecycle of the SUT.

3.1 Model Based Testing

The idea behind model-based testing (MBT) [22] is the representation of the SUT, the environment and its behaviour as well as the test itself by means of a model. Following this idea, model-based security testing (MBST) [23] verifies security properties of a software system through the model of the SUT. Therefore, MBT has the flexibility to test functional requirements and check implementation errors, to verify if the security checks are sufficient in case of an attack, and also to model attacks or check how the system reacts.

To perform MBT (and MBST), first, it is necessary to design the model from the system specification using a high-level representation. Here, languages such as UML [22], Object Constraint Language (OCL) [24] or domain specific languages (DSL) [25] can be employed. The model comprises the architecture of the system and the relation between other components. Second the test steps are specified based on the designed model, also following the high-level representation. Third, the tests can be generated. As the model and the tests are at a high-level view, a process is necessary to link the abstract model with the real system. The result of this process is an adapter, an interface in charge of translating the abstract language to a concrete command for a specific implementation. Once the adapter is implemented, the tests can be executed and the results can be analysed to determine if the tests have been passed or not.

One of the main advantages of MBT is the possibility of generating the tests in an automatic way from the SUT model. There are several tools [26] that help in this process such as CertifyIt [27] or MISTA[10]. Despite this benefit, human interaction is still needed to design the model, specify the tests and implement the adapter, which is, in general, very time consuming, and has a high learning curve. However, in case of recertification, the tests can, under some circumstances, be executed automatically, and the adapter can be extended if more tests are needed.

[10] http://cs.boisestate.edu/~dxu/research/MBT.html

3.2 Regression Testing

Regression testing [28] is mainly used to test changes over the SUT, verifying that there are no collateral effects and it provides the expected functionality correctly. Therefore, when the product is updated or patched, or when the product has been modified due to new requirements, regression testing is necessary. In security, regression testing is especially relevant when a new vulnerability is discovered and/or when a security patch is needed to solve a security issue. As the approach is complementary to other testing techniques, the level of abstraction will depend on it and on the level desired by the tester.

There are five main regression testing approaches [29] depending on the depth of the testing process: test all, reduction, minimisation, prioritisation and selection. The first one, test all, consists of repeating all the tests completely. This is the least efficient approach, as the process can be expensive and time consuming. The rest of the approaches try to reduce the number of tests executed, selecting a subset of relevant tests to perform the process in an efficient way. Minimisation consists of reducing the testing coverage, by removing some tests that are not relevant for the changes. Prioritisation orders the tests following specific criteria. The more relevant tests are executed first. Finally, selection chooses a subset of tests directly connected to the changes made on the product.

There are tools that facilitate the automation of regression testing. The paper [30] presents an extension of the CertifyIt to support regression testing.

3.3 Code-Based Testing

Code-based testing [31] is a white-box technique to detect vulnerabilities and faults by looking at the source code, in order to detect anomalies at the very early stages of the development. Code reviews can either be manual, where an expert reads program code line-by-line [32], or automated (e.g., static code analysis (SCA) or static application security testing (SAST) [33]). In SAST, a tool reviews the application code and automatically reports potential security flaws. It can use syntactic checks such as calling insecure API functions or using insecure configuration options. It is also possible to use semantic checks that require an understanding of the program semantics, such as the data and control flows.

While manual code reviews are a tedious process that requires skill, experience and persistence, SAST tools can analyse all control flows of a program in a scalable way. Based on that, these tools can provide detailed recommendations to fix security issues very early in the development process. Compared to dynamic test approaches, SAST tools provide a higher coverage and a lower false negative rate. However, these tools only report known vulnerabilities, and therefore, an expert is needed in order to configure the tool and identify such vulnerabilities.

3.4 Penetration Testing

Penetration testing [34] is a testing approach in which the SUT is tested from the outside. The setup is comparable to an actual attack from a malicious third party. The tester is only able to interact with the SUT using its public interface. Penetration testing can be black-box if the attacker has limited information about the system or white-box if the attacker has complete information about it. Penetration tests are commonly done for applications that are open for networked communication. Although penetration testing tests missing functionality or side-effects of the system, sometimes the target is the environment of the SUT (e.g., exploiting an unpatched operating system). In this sense, the effectiveness of the approach depends heavily on the requirements of what has to be tested. Going outside of the defined framework for penetration testing is considered bad practice and usually is strictly forbidden.

Although penetration testing is often performed manually, there are tools that help discover weaknesses in an automated way, such as port or vulnerability scanners [35] used to identify security issues in applications through various techniques. The scanner queries the application interfaces with a set of

predefined attack payloads and analyses the responses of the application for indicators if the attack was successful and, if this is not the case, hints how to alter the attack in the subsequent tries.

Moreover, several standards for penetration testing exist, among which the Open Source Security Testing Methodology Manual (OSSTMM) [36] is the most prominent one, providing rules and guidelines and covering all the Internet layers. The OSSTMM methodology covers the whole process of risk assessment involved in a penetration test, from initial requirements analysis to report generation.

However, penetration testing is usually difficult to perform, as the tests do not often directly cause observable security exploits. Furthermore, the security evaluator has to think like an attacker, which requires a high level of skills and expertise.

3.5 Fuzzing Testing

Fuzzing testing [37] is based on the idea of testing the SUT security flaws by using unexpected or erroneous inputs. This technique has been proven to be effective in finding vulnerabilities that are not considered by other techniques. Fuzzing testing can be performed over input data (data fuzzing testing) [37] by generating random input data, or over a message sequence (behavioural fuzzing testing) by sending valid or non-valid message sequences. Fuzzing testing is considered a black-box type of testing as it is not necessary to know the implementation details of the SUT. Also, as in penetration testing, its effectiveness depends on the requirements of what has to be tested.

Fuzzing testing makes use of a fuzz generator or fuzzer to generate the data. It can use various strategies for data generation. Random fuzzing is the more basic fuzzing approach as the data is generated randomly, without any conditions [37]. Mutation-based fuzzing testing [38] uses a mutation algorithm to generate variants of the known data, whereas model-based mutation testing [39] mutates the attack model, generating different paths to execute the attack and stress the system. Model inference assisted (MIA) evolutionary fuzzing testing [40] is focused on detecting cross-site scripting vulnerabilities combining model inference and genetic algorithms.

Although fuzzing testing has shown its benefits in terms of discovering zero-day vulnerabilities, the high number of tests generated poses scalability problems, making necessary its limitation, and therefore reducing its effectiveness. In addition, the implementation of a fuzzer can be cumbersome in some domains. Despite these challenges, large-scale and continuous fuzzing deployments like Google's OSS-Fuzz[11] or Microsoft's OneFuzz[12] are used with significant number of bugs found.

[11] Google, OSS-Fuzz. https://google.github.io/oss-fuzz. April 2021
[12] Microsoft, OneFuzz. https://github.com/microsoft/onefuzz. April 2021

4 Risk Assessment Approaches

This section reviews the main security risk assessment approaches that could be used in security certification to estimate and measure the risk. Even though not all certification schemes (e.g., CC) require risk assessment to be included in the process, we feel that estimating and measuring the risk of different threats occurring helps choose and prioritise the testing methods used.

Following the definition of CNSSI-4009, risk assessment is “the process of identifying, prioritising, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organisational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur”. Hence, we consider that a risk assessment methodology determines the risk of a vulnerability, weakness or threat, with the aim of measuring the security of a product, process, person or organisation and, therefore, of being able to compare different products.

Like in the certification schemes, there is a plethora of risk assessment mechanisms taking into account different metrics and procedures, which makes it difficult to compare different devices and systems assessed under different methodologies. In addition, some of the metrics considered, such as likelihood or impact, are difficult to be measured without previous attack logs. As a consequence, the overall process adds a certain degree of subjectivity.

Despite these issues, risk assessment provides a valuable tool to prioritise the tests to be executed during the certification process, as evaluating a system against all the possible vulnerabilities could be very time consuming and useless. Identifying which are the most important requirements or the most critical vulnerabilities can help to establish a priority list. Moreover, risk assessment allows to establish a qualitative measure of the risk associated with an encountered vulnerability, analysing its criticality taking into account additional aspects crucial in complex systems, such as the cascade effects between vulnerabilities or components, or the influence of the context in which the system operates.

4.1 The Common Weakness Scoring System (CWSS)

The Common Weakness Scoring System (CWSS) [41] is used to assign a numerical risk to software vulnerabilities. To do so, CWSS combines three groups of metrics that are used to calculate the risk: base finding, attack surface and environmental. The base finding metric group is focused on the inherent risk of the vulnerability, the confidence of the finding and strength of controls. However, metrics such as likelihood are difficult to compute [42]. The attack surface metric group includes the barriers that an attacker must overcome in order to exploit the weakness. Finally, the environmental metric group is related to the characteristics of the vulnerability specific for a domain.

Each factor in the metric groups is assigned a value, which is converted to its associate weight. The metrics of each group are calculated and combined with the other groups (multiplication) in order to obtain a complete risk measure, which ranges between 0 and 100. The base finding subscore is between 0 and 100, whereas the other ones can range between 0 and 1.

If the set of values proposed for the technical impact metric (including confidentiality, integrity and availability) is not precise enough, CWSS users can apply their own quantified methods to derive a subscore. One of the methods uses the Common Weakness Risk Analysis Framework (CWRAF) [43] to define a vignette and a technical impact scorecard. Here, vignette-specific importance ratings are used to calculate the impact weight. CWRAF and CWSS allow users to rank classes of weaknesses independent of any particular software package, in order to prioritise them relative to each other (e.g., "buffer overflows are higher priority than memory leaks"). This approach, sometimes referred to as a "top-n list," is used by the CWE/SANS Top 25 and OWASP Top Ten.

The main advantage of CWSS is that it allows unknown values when the information is incomplete, so it can be applied earlier in the process, before any vulnerability has been proven.

CWSS is recommended by the ITU-T in X.1525[13] and it is used in several vulnerability databases such as the Common Weakness Enumeration (CWE)[14] or the OWASP Top Ten[15].

4.2 The Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) [44] is an open framework for communicating the characteristics and severity of software vulnerabilities, similar to CWSS. It also consists of three metric groups: base, temporal and environmental. The base group represents the intrinsic qualities of a vulnerability, the temporal group reflects the characteristics of a vulnerability that change over time, and the environmental group represents the characteristics of a vulnerability that are unique to a user's environment, leading with the context influence challenge.

The base metrics produce a score ranging from 0.0 to 10.0, which can be modified by scoring the optional temporal and environmental metrics (they include a metric value that has no effect on the score). The current version of CVSS (CVSSv3.0) was released in June 2015. In the CVSSv3.0, the base metric group is composed by the access vector, access complexity and privileges required metrics. These capture how the vulnerability is accessed and whether or not extra conditions are required to exploit it and the three impact metrics (confidentiality, integrity and availability) that measure how a vulnerability, if exploited, will affect the vulnerable component. The temporal metrics include technical details of a vulnerability, the remediation status of the vulnerability, and the availability of exploit code or techniques. Finally, environmental metrics capture the characteristics of a vulnerability that are associated with a user's IT environment. Although CVSS is similar to CWSS, some metrics like likelihood have been removed, leading to metrics that are simpler to compute.

CVSS has been widely adopted, especially the use of base scores from the base metric group and it represents a widely established approach. For example, it is used in the Common Vulnerabilities and Exposures (CVE)[16] and in the National Vulnerability Database (NVD)[17] created by NIST.

4.3 DREAD

The DREAD algorithm [45] is used to compute a risk value, which is an average of five categories: damage potential (how great is the damage if the vulnerability is exploited?), reproducibility (how easy is it to reproduce the attack?), exploitability (how easy is it to launch an attack?), affected users (as a rough percentage, how many users are affected?) and discoverability (how easy is it to find the vulnerability?). It has been used at Microsoft and is currently used by OpenStack [46]. The context is not considered itself, but it can be taken into account when assigning the mark to each category. The same happens with the multilayer and complex systems, although an aggregation is not directly considered, it can be taken into account in the scale, as a global value.

The calculation always produces a number between 0 and 10; the higher the number, the more serious the risk. However, there is no consensus on how the actual risk point scale should be, since it all depends on the individuals performing the threat modelling [47]. DREAD requires scoring each of the five categories on a scale from zero to ten, which leads to discussions on the fine differences between consecutive numbers, e.g., five and six. This problem is even bigger in larger organisations with multiple

[13] https://www.itu.int/rec/T-REC-X.1525/en
[14] https://cwe.mitre.org/index.html
[15] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[16] https://cve.mitre.org/
[17] https://nvd.nist.gov

teams. One solution, as remarked in [48], is using scores of high, medium or low, that are easy to agree, instead of using the eleven-valued scale. For example, a simple scheme would be: high (10 points), medium (5 points), and low (0 points) when it comes to damage potential. Similarly, the scheme would be: hard (0 points), medium (5 points), easy (10 points) when it comes to reproducibility.

4.4 The Open Web Application Security (OWASP) Risk Rating Methodology

The Open Web Application Security (OWASP) Risk Rating Methodology [49] is part of the OWASP project, which provides a basis for testing web application technical security controls. The risk rating methodology estimates the risk in terms of likelihood and impact following several steps.

The first one consists on identifying a risk to be rated, analysing and gathering information about it. The second step analyses factors for estimating likelihood. It is not necessary to be over-precise in this estimate. Generally, identifying whether the likelihood is low, medium, or high is sufficient. There are a number of factors that can help determine the likelihood, such as the ease of discovery and exploit or the skills of the attacker.

The third step is about identifying factors for estimating impact. This is divided into technical impact (on the application, the data it uses, and the functions it provides) and into business impact (on the business and company operating the application). The context factor can be considered through this metric.

The fourth step determines severity of the risk. The likelihood and impact estimate are put together to calculate an overall severity for the risk, obtaining none, low, medium, high or critical. Finally, it is decided what to fix. It is also possible to customise the risk rating model by, for example, adding factors, customising options or weighting the factors.

The main limitation of OWASP is that it is only focused on web applications, a domain in which there is no current standard [50]. As in the other schemes, the scale used (low, medium and high) is based only on the consensus of the testers and as such makes the result subjective and variable depending on the person who is measuring the risk. Although a high precision on calculating the likelihood is not required, this is one of the metrics that is more difficult to compute. Finally, although multilayer and aggregation are not considered directly, they can be included by considering a global mark.

4.5 The Veracode Rating System

The Veracode Rating System [51] is an adaptation of CVSS to evaluate detected weaknesses/vulnerabilities. Veracode assigns a severity level to each flaw based on confidentiality, integrity, and availability. Each severity level reflects the business impact if a security breach occurs in these three security aspects.

The overall security quality score, based on its associated CWE entry, is computed by aggregating impact levels of all weaknesses within an application. Multilayer and aggregation are considered in this way. It ranges between 0 and 100, where 0 is insecure and 100 means that no flaws have been discovered. This score does not predict vulnerability potential as much as it enumerates the security weaknesses and their impact levels within the application code.

The score calculation includes non-linear factors so that, for instance, a single Severity 5 flaw is weighted more heavily than five Severity 1 flaws, and so that each additional flaw at a given severity contributes progressively less to the score. The weights are exponential and calculated empirically by the application security experts of Veracode, meaning that they can be affected by personal judgement. Finally, the score is normalised to a scale of 0 to 100, where 100 means no flaws have been detected [52].

The assurance levels follow a three-letter rating system (from A to F). The first letter is used for the results from source code analysis, the second for automated dynamic analysis, and the third for human testing. They are used to determine the extension of the testing (e.g., higher assurance levels could imply

more testing techniques) and the overall acceptance criteria (e.g., a lower assurance level can be accepted with lower security scores if it does not pose a high business risk).

4.6 Cenzic HARM (Hailstorm Application Risk Metric)

The Cenzic HARM [53] [60] (Hailstorm Application Risk Metric) is a quantitative score for risks associated with web applications. The metric is split into 4 impact areas relevant to web application security: the browser, the session, the web application, and the server. It also takes into account two additional factors (complexity and the precision associated with detection of a given vulnerability) and a modifier called weight, with which users can modify the obtained risk. However, this method does not account for the relationship of vulnerability properties, which are also important in the evaluation of the distribution of exploitation, and it is focused only on web applications.

Mathematically, the base risk equation is $10 * 2^I$, where I is the impact area value. Any vulnerability can impact a web application in up to 4 different ways (4 impact areas). Within those 4 areas, the degree of the risk can be 1 (“low”) to 5 (“critical”), represented as rings inside a circle. To determine the application risk level (impact value) for a vulnerability, HARM uses security values with five degrees of risk such as confidentiality or access. The vulnerability risk is the sum of the risk score from each of the four impact areas, which can be modified by the weights from other metrics (e.g., attack complexity or detection precision). Finally, the HARM rating is calculated by multiplying all of the identified vulnerabilities (that can include different components and layers) within an application by the level of importance managers give to that application, so it gives the possibility of indirectly considering the context changing the weights.

4.7 Modular Risk Assessment

The basis of modular risk assessment (MoRA) [54] is the determination of individual protection objectives, that is, those parts of a system that are particularly worth protecting. This determination requires close coordination with the respective company to better apply the risk analysis to the specific system. The methodology has been also applied in the context of smart vehicles, as it provides a high flexibility, also supporting hierarchical decomposition of the target of evaluation.

In particular, MoRA comprises four main activities: document TOE, determine protection needs, analyse threats, and analyse risks. Threats as well as possible controls are analysed based on catalogues of known threats or vulnerabilities and countermeasures. Then, threats are connected with components or data flows and evaluated based on risk factors like time, access, knowledge and equipment. These activities are supported by a proprietary security analyst tool[18]. The objective is to evaluate the security of existing systems using a risk model in a uniform, comparable and understandable way and to propose measures to minimize the risk. The tool provides a set of guidance artifacts such as an assessment model or a risk assessment template that can be used to specify a particular assessment model. This results in an estimated likelihood of risk. The methodology itself just gives the indication on the steps that should be performed but it does not give indications on what tools or approaches can be useful to instantiate it beyond the proprietary tool developed for it. Moreover, the tool does not provide a high automation of the processes, as the user is in charge of modelling, specifying the risks and selecting the mitigation. Finally, the methodology is based on the expert's opinion to quantify the risk instead of relying on security testing to validate the compliance of the security objectives.

[18] https://at.projects.genivi.org/wiki/download/attachments/7012490/MoRA Presentation for GENIVI Sec Team.mp4

4.8 Threat, Vulnerability, and Risk Analysis (TVRA)

Threat, vulnerability, and risk analysis (TVRA) [55] is an assessment method developed by the European Telecommunications Standards Institute (ETSI) developed for data and telecommunication networks.

The TVRA method can briefly be summarized as follows. First, the TOE, the associated assets (physical, human or logical) and the goals of the evaluation are identified. Security objectives are then identified and classified based on the five security attributes: confidentiality, integrity, availability, authenticity, and accountability. From them, we can derive the functional security requirements, which are more detailed requirements than the security objectives, e.g., passwords should be used for authentication. An inventory of assets is done and possible vulnerabilities are identified and classified along with corresponding threats and undesirable results. These threats are classified according to the following four categories: interception, manipulation, denial of service and repudiation. The risk is calculated based on the likelihood of these threats and their undesirable results. Finally, a set of countermeasures are derived and a cost-benefit analysis is carried out to select the most appropriate countermeasures to reduce the risk of the identified threats. These results are then used to design security services. However, the standard only gives the steps to be performed, not how to perform them.

5 Challenges of Certification

This Section reviews the main challenges associated with the cybersecurity certification process.

5.1 Heterogeneity of Existing Certification Schemes

One of the main challenges associated with security certification is the harmonization of the wide variety of security certification schemes that coexist together [56]. The current heterogeneity makes it difficult to compare different solutions and processes, especially when a product is evaluated under different certification schemes at national levels. Currently, there is no unified solution that copes with these issues; therefore, the process of comparing and assessing the cybersecurity level of different products is challenging.

ENISA has already remarked the need for harmonization of security certification at least at the European level, which could help to increase the trustworthiness and competitiveness of European products [57]. Following the recommendations of ENISA, there are some elements that should be harmonized. This is the case of the different assurance levels, the elements considered during the certification process and the roles of the involved stakeholders.

Regulatory bodies have an important role here, promoting the creation of a cybersecurity framework through the consensus of the main stakeholders and orchestrating its development and deployment. In particular, the certification meta-scheme proposed by ECSO [58] represents an ambitious initiative to homogenise and aggregate different certification approaches under a common framework.

At the legal level it is possible to distinguish at least two levels of cybersecurity certifications:

1. A European cybersecurity certification scheme is a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes;

2. A national cybersecurity certification scheme is a comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority and that apply to the certification or conformity assessment of ICT products, ICT services and ICT processes falling under the scope of the specific scheme.

Schemes at the different levels can, however, be very heterogeneous, the schemes difficult to compare and, in extreme cases, even contradictory.

5.2 Lack of Standardisation for the Certification Process

In spite of the limitations of the current certification approaches, a cybersecurity certification scheme should be based on the main concepts and operational aspects of existing standard (such as Common Criteria (CC) [1]). Most of current initiatives try to use the same concepts and terms that were defined by these approaches. The use of standardised approaches will enable a common understanding about the implications and requirements of cybersecurity certification, and it will help to provide a more harmonised view of certification in different contexts, domains or countries. Indeed, this aspect is especially relevant in the IoT domain, which is characterized by a still fragmented landscape of standards. We believe that the alignment of current certification schemes is crucial to foster a homogeneous perspective on IoT cybersecurity.

In addition, the current heterogeneity of risk assessment approaches hinders the adoption of current schemes in the IoT paradigm. Indeed, beyond the different approaches for risk assessment, we noticed

a lack of common consensus and standards to refer the concepts related to the risk assessment process itself [59]. In this direction, we believe that the adoption of a standard-based common framework for security risk assessment is crucial to foster a homogeneous perspective on cybersecurity risks in IoT.

5.3 Complexity of the Certification Process for Product Lifecycles

Existing approaches are usually expensive, slow and complex [60], [4]. This could imply that an organisation, especially an SME, might not be able to afford the costs of the certification process, or even cause a delay in the market release of the product leading to a loss of revenue.

Cybersecurity is a very dynamic concept and validity of a security certificate has to reflect that. Taking into account the frequency of updates and patches of certain products, a lightweight recertification process is necessary to ensure an updated security certificate. Automated procedures are also necessary to ensure the scalability of the (re)certification process. In this sense, the cybersecurity certification scheme should deal with the changes of or appendices to the certificate. On the one hand, the product should be monitored during its lifecycle in order to detect new vulnerabilities and update its security level accordingly. On the other hand, the security level should be reconsidered when recertification is required due to an update/patching. For example, the certifying body may request post-market surveillance reports and void the certification if these are not prepared over a certain period of time.

5.4 Composition of Certified Properties for Combined Systems

Another issue is that a system could contain several components with different levels of security. Security composition is a desirable design feature in cybersecurity certification and deployment at least for some security properties (e.g., confidentiality, authentication), but it is usually hard to perform in a way that all the layers and threats are correctly weighted [61]. The security certification process should also take into account the protocol stack to cover vulnerabilities at different layers. Indeed, the RASEN project [62] proposes a mechanism to aggregate risks from different layers. However, physical aspects remain as a challenge due to the context dynamicity, which means that security properties are difficult to separate from other layers of a component. Additionally, the components of a certified item might not be clearly identified or not suitable for automatic processing. A mapping of the certified item to the records in the existing vulnerability databases, like common vulnerabilities and exposures (CVE) via the item platform identifier, is sometimes non-existent or ambiguous, making it harder to automatically obtain and list existing vulnerabilities, especially for composite cases.

5.5 Communicability of Certification Results to the End User

The transparency of the cybersecurity certification results to the end user is a common problem as the user may not easily perceive the positive results of the security evaluation due to the complex jargon of security certification processes. The negative consequence is that the user fails to understand the added value of the cybersecurity certification thus decreasing the appeal of such process in the market. As a result of the certification process, a label should be generated to provide a simple, clear and visual level(s) of the security being certified [63]. Companies such as Bosch [64], add that customers need to compare the security of different products without feeling overwhelmed with technical details. In this sense, the label has to address an important trade-off between the simplicity of the label and the non-ambiguous and complete representation of the results of the process. This is rather difficult, because in comparison to the energy label, which measures a physical quantity, the measurements of security are far more complex. In addition, the label design should also take into consideration the dynamicity of the

security. As pointed out by ECSO WG1[19], a visual static cybersecurity label is not enough, since it should also cope with the dynamism of security threats and context to reflect changes in the current security level. For this reason, the usage of an NFC or a digital QR code, which can be regenerated, can help to check the status of the cybersecurity label in a fast an easy way, as it could also be easy to update. However, this may have other security issues such as the possibility to falsify the information.

5.6 Comparability of Certification Levels

The context in which the product will operate must be considered, in order to make products comparable among each other and to specify the boundary conditions of the context where the cybersecurity certification was applied. This aspect is specially challenging, because it could not be known *a priori*.

To address the issue of label significance and the need to measure the security properties, security metrics must be established. However, some of such metrics, such as likelihood or impact, are difficult to measure[20], due to their complexity, which was reported in [65] already in 2004. Nevertheless, year 2020 saw the highest number of certified items under the Common Criteria scheme with almost 350 items compared to only around a hundred items in 2004.

In addition, certification or security levels, even in case of certification, might not always be comparable. In Common Criteria, for example, comparability is only achievable for assurance requirements, not functional ones. The situation is further complicated by the potentially uneven level of scrutiny by evaluation facilities. However, Protection Profiles as the standard templates for a specific product domain (e.g., firewall functionality) and their overall increased adoption (large majority of new certificates are now certified according to PP) now improve comparability.

5.7 Relations with Data Protection Regulation

Cybersecurity provides controls for data protection, but organisations require additional considerations to satisfy privacy goals. For example, while cybersecurity protects the assets of the organisation from security incidents, privacy goals require the organisation to rethink how many assets it should have from natural persons (minimisation) and how they are processed (transparency).

Still, certification is an important tool to demonstrate compliance with the GDPR. In this context, it can be understood as a means to:

1. demonstrate compliance with the provisions on data protection by design and by default (GDPR article 25(3));
2. demonstrate that an appropriate technical and organisational measure is put in place to ensure data security (GDPR article 32(3)); and
3. to support transfers of personal data to third countries or international organisations (GDPR article 46(2)(f)).

[19] https://www.ecs-org.eu/working-groups/wg1-standardisation-certification-labelling-and-supply-chain-management

[20] https://www.usenix.org/legacy/event/hotos09/tech/full_papers/arnold/arnold_html/ and https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1294&context=amcis2009

5.8 Accreditation of Certification Bodies

To achieve trustworthy certification, we need reliable, competent, and independent bodies carrying out the certification. One way to achieve this, is to require the certifying bodies to be accredited. This is required, for example, by article 43 of GDPR for certification bodies that provide data protection certification. This accreditation can usually be carried out by a national accreditation body if they have the competence in the necessary field. However, in a smaller member state, this might not be the case. This adds another layer to the certification process on the member state level and can increase the cost of certification, if an accreditation body is not locally available for the field in question. Another example of complications due to accreditation is when a new standard has taken effect but the rules for accreditation have yet to be developed, however, certification should already be done with the new standard in mind. The situation is further complicated, if the certification body is not performing the certification in-house, but instead relies on accredited evaluation facilities as, for example, for FIPS or Common Criteria certifications.

6 The Role of the European Union Cybersecurity Act

The European Union Cybersecurity Act is expected to make a strong push in Europe towards satisfying several of the challenges in cybersecurity certification. For example, it will address the need to bring different certification schemes under a common framework in order to avoid the risk of fragmentation and barriers in the European Digital Single Market. As it is underlined in the text of the EU Cybersecurity Act[21]:"An increase in trust can be facilitated by union-wide certification providing for common cybersecurity requirements and evaluation criteria across national markets and sectors".

In order to facilitate the creation of a common European framework, the EU Cybersecurity Act provides for the establishment of the Stakeholder Cybersecurity Certification Group[22]. "The Stakeholder Cybersecurity Certification Group should be established in order to help ENISA and the Commission facilitate the consultation of relevant stakeholders. The Stakeholder Cybersecurity Certification Group should be composed of members representing industry in balanced proportions, both on the demand side and the supply side of ICT products and ICT services, and including, in particular, SMEs, digital service providers, European and international standardisation bodies, national accreditation bodies, data protection supervisory authorities and conformity assessment bodies pursuant to Regulation (EC) No 765/2008 of the European Parliament and of the Council, and academia as well as consumer organisations."

The EU Cybersecurity Act provides that the EU approved certification schemes will specify:

1. the categories of products to be covered,
2. the cybersecurity requirements for each (referencing standards or technical specifications),
3. the type of evaluation required (self-assessment or third-party evaluation),
4. the intended level of assurance (basic, substantial or high).

Therefore, we expect that the effort driven by the act will contribute significantly towards several of the challenges of certification, including heterogeneity and co-existing national schemes (Subsection 5.1), complexity (Subsection 5.3), communicability (Subsection 5.5) and comparability (Subsection 5.6). The rest of the challenges discussed in Section 5 are expected to benefit from additional research in the domain.

[21] EU Cybersecurity Act. Recital (7) https://op.europa.eu/sl/publication-detail/-/publication/35e93bb4-8905-11e9-9369-01aa75ed71a1/language-en

[22] EU Cybersecurity Act. Recital (62) https://op.europa.eu/sl/publication-detail/-/publication/35e93bb4-8905-11e9-9369-01aa75ed71a1/language-en

7 Virtual Cybersecurity Certification Centre

7.1 Overview

Cybersecurity is recognised to be a crucial component but also a frequent weak point for current software systems, devices, services, and cyber-physical systems. Over time, various certification schemes like Common Criteria, NIST FIPS140-2, EMVCo, or PCI Security Standards were designed and implemented for the specific usage domain.

This deliverable and Deliverable 8.4 provide an overview of the existing security certification and security standardisations schemes, frameworks, and organisations. As extensively documented in these deliverables, the introduction of new certification or standardisation scheme is a non-trivial task, requiring domain-specific knowledge and technical, organisational, and procedural support from a majority of the stakeholders involved. Only then the resulting certification artifacts are possibly widely recognized and functional and improve the security of the items assessed.

While the analysis of the existing certification schemes identified shortcomings and limitations, a design of a new virtual certification framework would be practically impossible to turn into the practices used, well-known, mature, and long-term maintained. Acknowledging this fact, we instead proposed, implemented, and continue to operate a virtual cybersecurity certification centre operating on the principle of virtual overlay over the existing security certification schemes. The centre is available at https://seccerts.org and is interlinking corresponding available certification artifacts, information about a certified item extracted using data mining techniques, further enriched with additional metadata, preferably collected in a crowdsourced manner using open tools for easier sharing and distribution. By interlinking certified items between certification schemes as well as vulnerability databases, users of certified products can more accurately assess the target item before potential purchase and obtain possibly faster notification about the newly discovered vulnerabilities. The large number of the included items certified under existing schemes also allows for monitoring past and ongoing trends among the certified items and their categories.

The seccerts virtual certification centre is not competing with nor trying to replace existing certification schemes. The primary motivation for its use is the availability of functionality otherwise difficult to reach or not available at all within the current certification schemes – for example, automatic vulnerability notification in all components relevant for the product used or independent verification of the product delivered. Once used broadly, we believe that the additional information available via the virtual centre will positively influence the transparency of the underlying certification scheme(s) via increased power and insight of the end-users of certified products.

7.1.1 Involved Entities

Multiple entities are involved in the operation and usage of the virtual certification centre. We will briefly look at end-users, data providers, trust entities and developers.

The existing or potential future users of a certified product or analysts interested in the product scrutiny are interested in getting security-relevant up-to-date information about a product they use, verifying that the delivered product matches the certified etalon or other scrutiny of the product. End-user can be of different levels of sophistication with respect to the verification of the data provided by the virtual certification centre, starting from passive consumption of the information (e.g., notification about new related vulnerability), continuing with the use of open tools for analysis (e.g., listing the set of installed packages and checking the expected versions), and ending with the creation of new metadata about the certified device (e.g., power consumption traces captured via oscilloscope). End-users may also decide to outsource some analysis to contracted third-party entities (consultants, laboratories).

Data providers are entities providing the data and metadata aggregated by the virtual certification centre. The set of data providers is open and changes over time. The data provided is not automatically trustworthy and it is up to the end-users to determine how much they trust. The data can roughly be categorised as follows.

- Data produced during the certification process is the data already available as a part of the existing certification process. The data must be extracted from the original source format.
- Additional metadata can be added after certification using any relevant analysis tool (preferably an open-source tool to enable independent verification).

Trust entities are not a required part of the process. They are responsible for the selection of certification metadata which shall be used by a specific subset of end-users. As the set of data providers is generally open, end-users may decide to restrict accepted metadata only to parties authorised by their trust entity (e.g., relevant governmental agency). Trust entities are able to assess the validity of relevant metadata and authorise it by relevant means, e.g., digital signature.

Developers are responsible for the development of the core centre functionality. The development is performed in free and open-source software (FOSS) model. Developers are able to maintain the base code quality with respect to expected functionality. Due to the use of the FOSS model, multiple forks of implementation may arise in the future in case of stalled development of the original developers or dispute in the project direction.

7.2 Main Goals

The virtual cybersecurity certification centre was created with the following goals in mind:

- Added benefit building atop of existing certification schemes. The virtual centre utilises outputs from the existing certification schemes and public databases like Common Criteria, NIST FIPS140-2/3 or National Vulnerability Database (NVD). By processing, connecting, and overlaying from these data sources, additional insight is added instead of competing with them. The virtual centre is extensible to other schemes in the future.
- Open data and open tools approach for better transparency and accessibility. Open-source, freely available tools and data-driven approach is utilised to provide better accessibility for end-users by extracting the most relevant data otherwise hidden in certification documents. Open availability also increases the transparency of a whole certification process by making it easier to verify claims made and compare between different certificates.
- Provide deeper insight into certification ecosystem trends over the time. The certification process is typically evolving over time, with different actors adopting potentially different strategies during the certification procedure. Data-driven approach may provide insight into prevalent ways how items are certified, frequency of used certification claims (e.g., Security Functional Requirement (SFR), Security Assurance Requirement (SAR)), type of the items certified, used security and cryptographic mechanisms, and others.
- Provide faster notification to end-users in case of new potential vulnerability. Pairing of certified items and its dependencies (referenced certificates) with the platform identifier in the vulnerability database allows for push notification for relevant changes, like the occurrence of a new vulnerability, in the user-selected set of certificates.
- Provide better end-user verifiability of the purchased certified product. Despite a certified products being described in the certification documents (e.g., the target of evaluation), the end-user may have only limited options on how to verify if the purchased product is genuine. As the standard shallow identifiers (like Card Production Life Cycle data (CPLC) records for smartcards) can be easily tampered with, the virtual centre may host authenticated forensic profiles based on the harder-to-manipulate product behavioural properties (e.g., detailed performance profiling or power consumption traces) created by a trusted authority (e.g., evaluation laboratory) using open tools. User will later collect the same properties from the purchased product using the same open tools and compare them to the expected forensic template. Increased end-user verifiability shall increase the product scrutiny by performing repeated checks spread in time (instead of single-time checks) and performed by many different users.

7.3 Basic Design and Implementation

The sec-certs suite of tools is developed as free and open-source project on GitHub [SECCERTS]. The project allows users to interact using the following interfaces:

- Web portal. The processed data and visualizations are available on the https://seccerts.org/ portal, allowing users easily search for and inspect included certified items and relevant linked metadata. No programming skills are required.
- Python SDK interface. The main programmatic interface to access data processing functionality is Python-based application programming interface. The Python SDK is typically utilised using existing Jupyter Notebook skeletons. Basic Python programming skills are required.
- Raw datasets. The processed datasets extracted from a raw source data like certification reports and technical documentation are available for any further analysis as json files. These datasets can be processed in any suitable programming language.
- Pull requests to extend/improve available datasets and code base. A user may provide additional overlay data sources using mapping files or improve the source code using standard mechanisms offered by git/GitHub.
- Local processing. Open availability of used tooling allows anyone to reconstruct processed results locally, with optional inclusion of non-public documents and other resources which are not available for https://seccerts.org/ portal.

The internal implementation of sec-certs suite of tools is described in detail in code documentation (https://seccerts.org/docs/index.html), here we summarize only the most important high-level modules:

- Monitoring of webpages like Common Criteria portal[23], NIST FIPS140
- Processing of pdf documents like certification reports, security targets, maintenance reports…
    - Basic certificate information (CC/FIPS, certificate id, scheme, vendor, evaluation labs…
    - Protection Profile used
    - Security target / security policy information
    - Extracted keywords (cryptography, security, device, standards…)
- Mapping to NVD vulnerability database, identification of corresponding Common Platform Enumeration (CPE) record, extracted information and connected CVE vulnerabilities.
- Forensic profile of certified device using open tools to extract device profile (now mostly cryptographic smartcards and Trusted Platform Modules).
- Visualisation of aggregated statistics
    - Visualisation of security assurance and functional requirements (SARs and SFRs)
    - Graph of references among related certificates
- Overlay mappings to process mapping between certified items and additional metadata sources bottom-up approach with metadata added by end-users.

The seccerts tool operates with incomplete and noisy input data, which may result in partially incorrect results (e.g., incorrect matching to NVD database). The inaccurate results can be addressed on multiple levels, including improvement of input data (see recommendations below), improvement of processing and heuristics used to include verification against additional sources and corrections based on the expert human inputs (feedback form on webpage, git pull requests…).

Figure 3 shows the basic web interface of seccerts.org overlay portal. So far, Common Criteria and FIPS140-2 certificates have been included. Figure 4 depicts an example summary page for the certified item Oracle Database 11g certificate. The basic information directly available from

[23] https://www.commoncriteriaportal.org/

commoncriteriaportal.org is shown including additional metadata extracted from certification documents like the certificate ID or the protection profile used. The warning banner notifies about the matched potential vulnerabilities. Figure 5 gives the details of the paired CPE entries to Oracle Database 11g certificate with displayed known CVE vulnerabilities. The virtual overlay connects the CC certified item with the NIST NVD vulnerability database. Figure 6 shows the graph of references to other certified items extracted from the certificate. Vulnerabilities in the referenced items may also affect the certified product. In Figure 7, it is possible to see the relevant keywords extracted from the security target document. Referenced CC Claims, Security Assurance Requirements (SAR), Security Functional Requirements (SFR) and other referenced standards are shown.

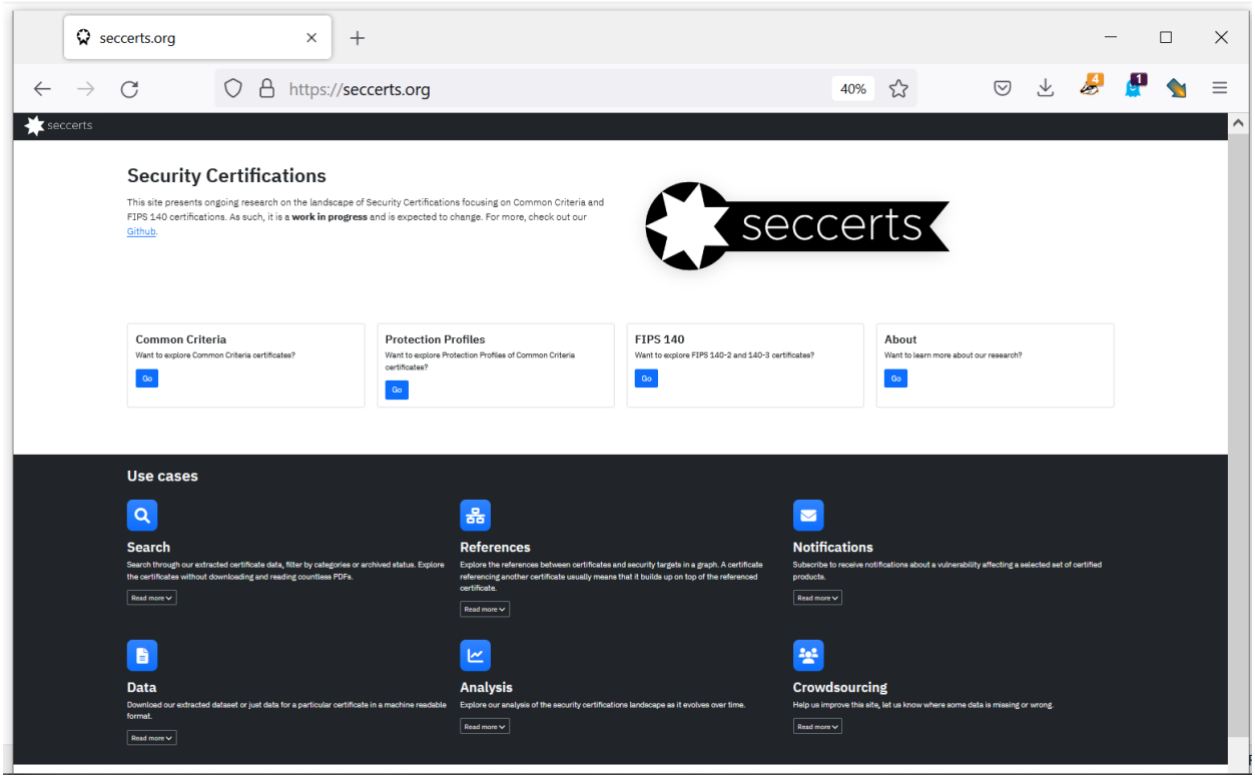

Figure 3 Basic web interface of seccerts.org overlay portal

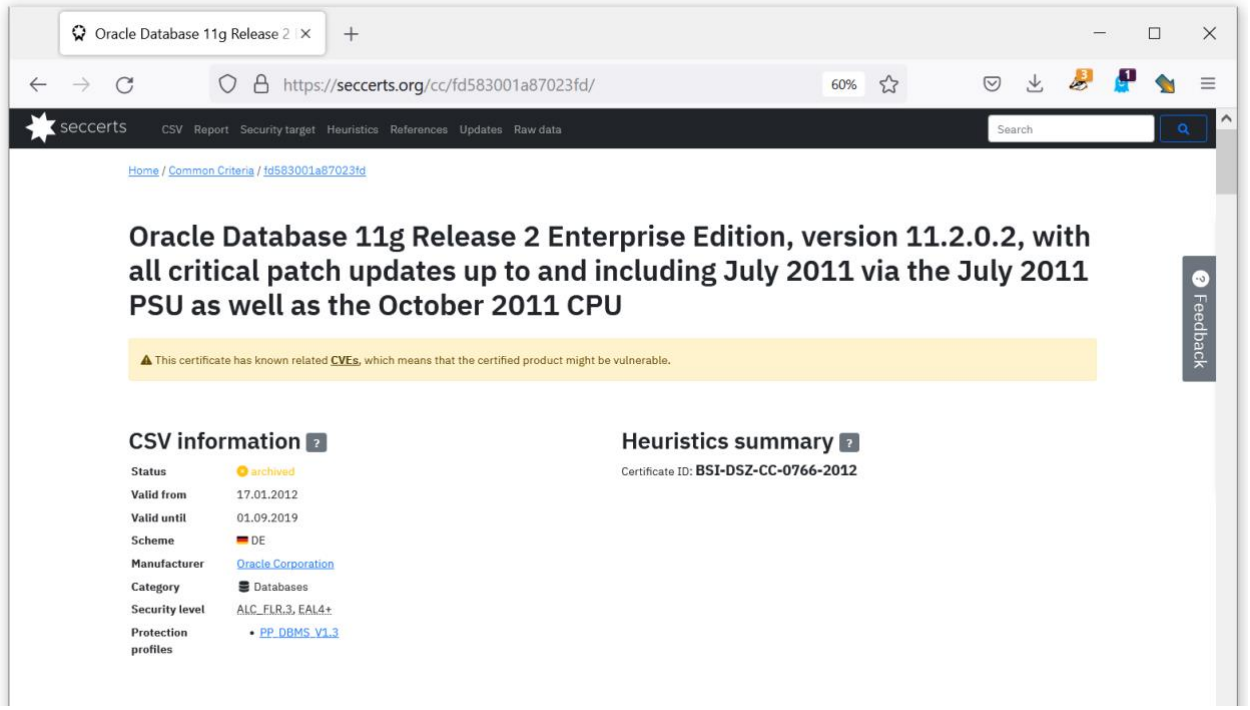

Figure 4 Example summary page for a certified item

Heuristics

Certificate ID: **BSI-DSZ-CC-0766-2012**

CPE matches

- cpe:2.3:a:oracle:database_server:11.2.0.2:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:database_server:11:*:*:*:*:*:*:*

Related CVEs

ID	Links	Severity	CVSS Score			Published on
			Base	Exploitability	Impact	
CVE-2003-0727	C M N	LOW	2.1		2.9	20.10.2003 04:00
CVE-2005-0297	C M N	HIGH	7.5		6.4	18.01.2005 05:00
CVE-2005-0701	C M N	MEDIUM	5.0		2.9	07.03.2005 05:00
CVE-2006-2081	C M N	MEDIUM	4.6		6.4	27.04.2006 23:02
CVE-2006-7141	C M N	MEDIUM	6.0		6.4	07.03.2007 20:19
CVE-2007-5510	C M N	MEDIUM	6.5		6.4	17.10.2007 23:17
CVE-2007-5511	C M N	MEDIUM	6.5		6.4	17.10.2007 23:17
CVE-2007-5554	C M N	HIGH	7.1		6.9	18.10.2007 20:17
CVE-2007-5897	C M N	HIGH	8.5		10.0	08.11.2007 21:46
CVE-2007-6260	C M N	MEDIUM	6.8		6.4	06.12.2007 02:46

Figure 5 Paired CPE entries with displayed known CVE vulnerabilities

Figure 6 Graph of references to other certified items extracted from the certificate

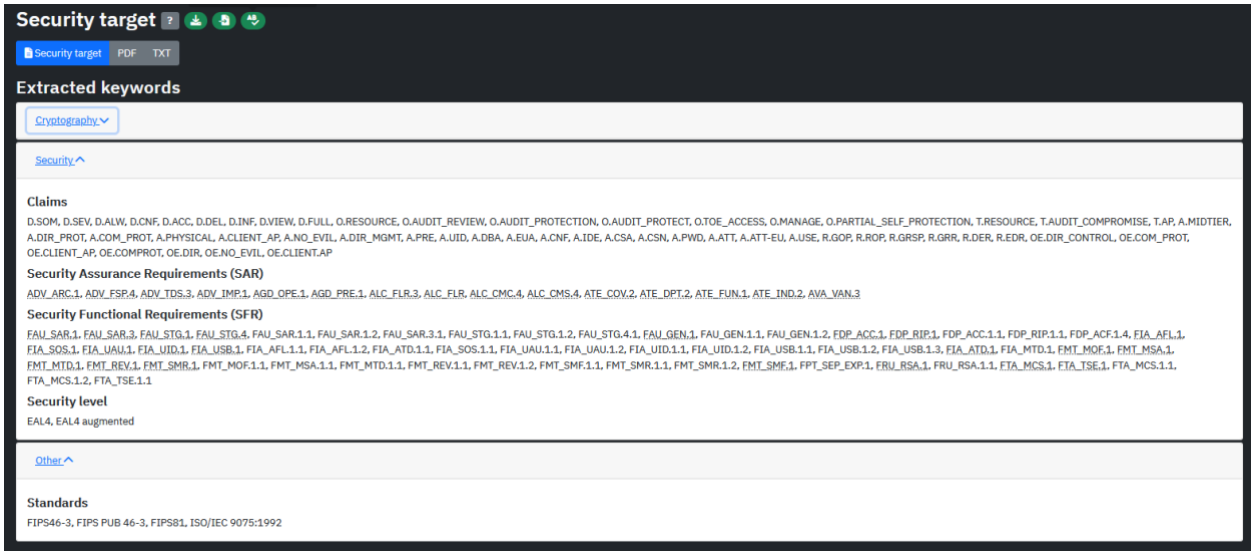

Figure 7 Relevant keywords extracted from the security target document

7.4 Governance and Operations

The sustained operation of the sec-certs virtual certification centre requires the means to 1) develop the initial functionality, 2) governance of future code changes, 3) governance of metadata additions, and 4) operate the necessary online services. While the initial functionality was implemented during the CS4E project, the remaining three parts require contingency planning to continue operation after the CS4E project is completed to prevent deterioration of the project value as well as prevent centralization and single point of failure as may happen in case of a single project operator. Below, we address these parts.

7.4.1 Governance for the Tool Source-Code Changes

The further development of project code to include new features as well as to update existing data processing pipelines requires coordination of the code updates. We use the standard open-source development model based on an upstream git repository (hosted on GitHub) with code changes proposed, analysed, and eventually merged via Pull requests. The repository maintainers with write rights are responsible for code review of the proposed changes. Such workflow is preferred to keep the changes at a single place (upstream repository), but also requires approval from the repository maintainers.

In case of repository' maintainers are not responsive or conflict of ideas about the tool's future direction arise (both commonly happening in a mature open-source ecosystem), the repository can be forked and developed in parallel to the original one. The sec-certs tool source code is intentionally open-source and

with a permissive MIT license to support other developers to develop their own modifications and resolve such conflicts of ideas.

7.4.2 Governance for the User-Added Metadata

The sec-certs tool forms the basis for the processing of additional datasets provided by external sources. The quality and trustworthiness of extracted, processed, and interpreted certification-related data depend on several factors influencing the resulting accuracy and relevancy. As the project is built as open and wants to motivate a wide range of users to provide additional community-based metadata, it may also receive incorrect inputs or inputs of insufficient quality. Some form of governance process is therefore required to filter the submitted metadata and/or enable end-users to decide which metadata are relevant for their use case.

We consider the following characteristics regarding the data accuracy and relevancy:

- Trustworthiness of original source data like CC certification report, security target, and other documents.
- Trustworthiness of the metadata extraction technique – as some extraction heuristics might be required, imprecise extracted metadata may be obtained.
- Trustworthiness of the connections between different records in the database – mapping between a particular certificate and its CPE entry in NVD database.

As the metadata provided may, in principle, come from any source, there is no level of assurance for their quality and trustworthiness. As a result, the end-user must decide which metadata is relevant and trustworthy enough. However, the existence of (standard) trusted entities is assumed to help the end-user with the decision together with technical support from the virtual certification centre tooling. Again, we utilise an open-source governance model adapted to handle the metadata to enable metadata filtering based on the input from trusted entities. The mapping between the certified items and relevant metadata is specified in structured mapping files, which are:

- **Openly available**. The mapping files are placed in a separate repository, versioned using git, and hosted on GitHub. Users can also create own mapping files from non-public metadata.
- **Extendable**. Similarly to the source code governance, the metadata submitter creates a pull request containing the mapping file (or change of an existing one).
- **Authenticated** (optional). The entities providing the metadata can cryptographically attest to the data provided (e.g., the power trace profile for a given smartcard generated by SCRUTINY module). End-user can take only a subset of metadata from trustworthy entities into an account using data mappings files.
- **Optional to use**. The virtual certification centre interconnects data sources and extracted metadata using data mappings files with open format. The data mappings can be provided by virtually anyone, and it is up to the end-user to select which mappings are relevant to its use case, resulting in a different output of sec-certs tool.
    - For example, community-provided data may have highest coverage but also less trustworthiness, e.g., due to lower quality of measurements.
    - For example, a national certification body (e.g., BSI) can define its own mappings for the devices certified under that scheme with additional metadata from the certification process. While not covering all CC-certified items, it may be considered more trustworthy for the items included.

7.4.3 Long-Term Operation of the Virtual Certification Centre

For the foreseeable future, CRoCS laboratory at Masaryk University plans to maintain the toolchain and resulting seccert.org portal. The process of database and related portal updates is automated.

The tools required to rebuild and set up the portal, including the extracted metadata, are available on GitHub, making it available centre by other entities or locally are available. In the spirit of free, open-source development (FOSS), the project can be forked and improved even if not maintained anymore by original developers.

The existing data mapping files are also publicly available in GitHub repository, making it easy to archive and/or extend directly by pull requests to the existing repository or indirectly by repository fork in case unmaintained repository.

Some parts of the processing pipeline require occasional updates in case of changes done on the source data side (e.g., CCPortal HTML/CSV format). Such breaking changes (out of our control) occurred several times already during the project development and are expected to happen again. However, the required changes to correctly process the new format of source data were usually minimal. The older processed datasets are still available even if newly added data (e.g., newly certified products) cannot be correctly extracted.

7.5 Advantages of the Virtual Certification Centre over the State of the Art

Our virtual certification centre mainly works to alleviate the lack of transparency and lack of communicability. By using structured evaluation reports and introducing dependency graphs, the virtual certification centre makes the certification results more transparent and simplifies the visibility of dependencies in case vulnerabilities are found in some underlying technologies.

In addition, our virtual certification centre is not another separate certification scheme but allows to use an existing scheme as the basis for certification. As such, it would be possible to use the combination of schemes that SURFACE (detailed in Deliverable 3.22) offers as the basis for certification and, hence, also lessen the complexity of product lifecycle certification.

8 Validation

8.1 Seccerts.org Usage Example: the ROCA Cryptographic Vulnerability

One of the motivations for this work was to improve the security assessment when a new vulnerability is found in a certified product. Such a utility is helpful to certification ecosystem stakeholders -- end-users can get early notification of potential vulnerability for the purchased products, security researchers can shortlist other items for further scrutiny, and responsible disclosure and product vendors can assess their certified products. Importantly, end-users are not dependent solely on the information flow from the vulnerable item vendor, which may have misalignment incentives for timely notification or may simply not be able to directly contact the end-user -- as is the case when a product is sold via intermediaries.

To demonstrate the future utility of seccerts methodology, we can retrospectively re-analyse past (known) vulnerabilities and compare the obtainable information with the mature understanding of the now past vulnerability. We cover algorithmic vulnerability in RSA keypair generation in Infineon cryptographic chips [66].

We would like to note that such evaluation is qualitative rather than a quantitative study. It is certainly easier to search for something already known to exist (affected products), a comparison might be biased due to the vulnerability type (we are investigating only several high-profile vulnerabilities) and affected item type (we focus on the domain of cryptographic hardware where we expect higher benefits due to overall ecosystem closeness).

8.1.1 Failed Notification of the Estonian Government (estID)

Timely notification of end-users about a vulnerability found, and the corresponding fix typically relies on the vendor or public sources like vulnerability databases. Such notifications may fail even for highly sensitive and certified devices, as demonstrated, e.g., by that of the Estonian government about the critical ROCA cryptographic vulnerability [66].

We use the case of Estonian eID documents utilising the vulnerable chip (certificate number ANSSI-CC-2013/55) as a use case. In short, after the responsible disclosure by original researchers to Infineon, the larger affected parties (which the Estonia government certainly is) were supposed to be notified before the public disclosure, either by the estID vendor or via non-public memos distributed among the parties involved in EU-wide eIDAS [67] directive. But the vulnerability information was received until the beginning of September, close to the national elections with electronic voting via vulnerable estID cards. While we cannot assess the information distribution via a direct vendor, we can analyse the information distributed in eIDAS incident report memo ID 163484 issued to all EU members on 20th June 2017 [68] by the affected Austrian e-health provider. That circulated memo did not alert Estonia

to become aware of the impact at the time. Figure 9 depicts the extracted metadata for the two certificates mentioned in memo ID 163484.

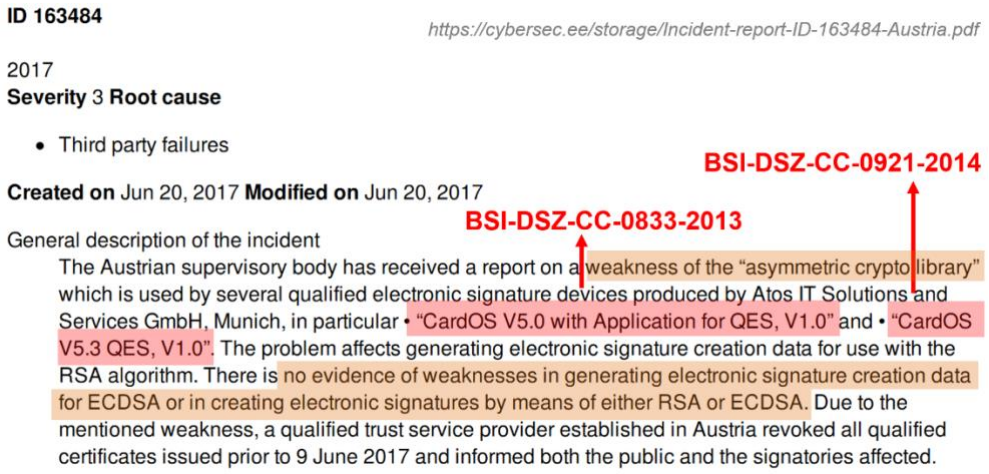

Figure 8 The relevant parts of the eIDAS memo ID 163484.

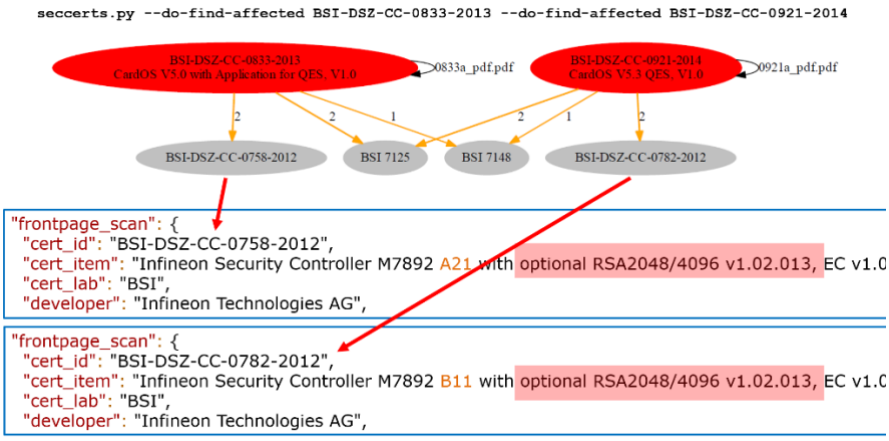

Figure 9. Extracted metadata for the two certificates mentioned in Memo ID 163484.

Out of the memo, one can read that ``CardOS V5.0 with Application for QES, V1.0" and ``CardOS V5.3 QES, V1.0" are vulnerable (directly corresponding to certificates BSI-DSZ-CC-0833-2013 and BSI-DSZ-CC-0921-2014). Also, ``weakness in asymmetric crypto library" and that ``problem affects generating electronic signature creation data for use with the RSA algorithm" were noted. While the concrete vendor was named, it was not the maker of the chip but the platform integrator instead. Using these two certificates, search for affecting items using --do-find-affecting BSI-DSZ-CC-0833-2013 BSI-DSZ-CC-0921-2014 returns a simple dependency graph based on the two chip certificates -- BSI-DSZ-CC-0758-2012 and BSI-DSZ-CC-0782-2012 -- both being version of Infineon Security Controller M7892 with ``optional RSA2048/4096 v1.02.013 ... libraries", matching the weakness description provided in memo ID 163484. Having vulnerable chip certificates, we can search --find-affected BSI-DSZ-CC-0758-2012 BSI-DSZ-CC-0782-2012 for certificates directly or indirectly referencing the vulnerable chip. More than one hundred certificates are found, but Estonia's ANSSI-CC-2013/55 is not among them (ANSSI-CC-2013/55 uses a different certified chip but with the same cryptographic library). To match also ANSSI-CC-2013/55, one needs to create the initial set of vulnerable certificates from all chips with RSALib v1.02.013 library and build a dependency graph from this set using --do-find-affected-keyword v1.02.013 - crucial insight which requires understanding what was shared between BSI-DSZ-CC-0833-2013 and BSI-DSZ-CC-0921-2014 and is also relevant to the description of weakness as stated in memo 163484. The automatic search alone would not be sufficient in this case, but easy refinement with input from a security expert is sufficient. Figure 10 shows the visualisation of

certificates relevant to a search based on a) Memo 163484 information and b) vulnerable library keyword v1.02.13. The colours correspond to different certificate issuing countries.

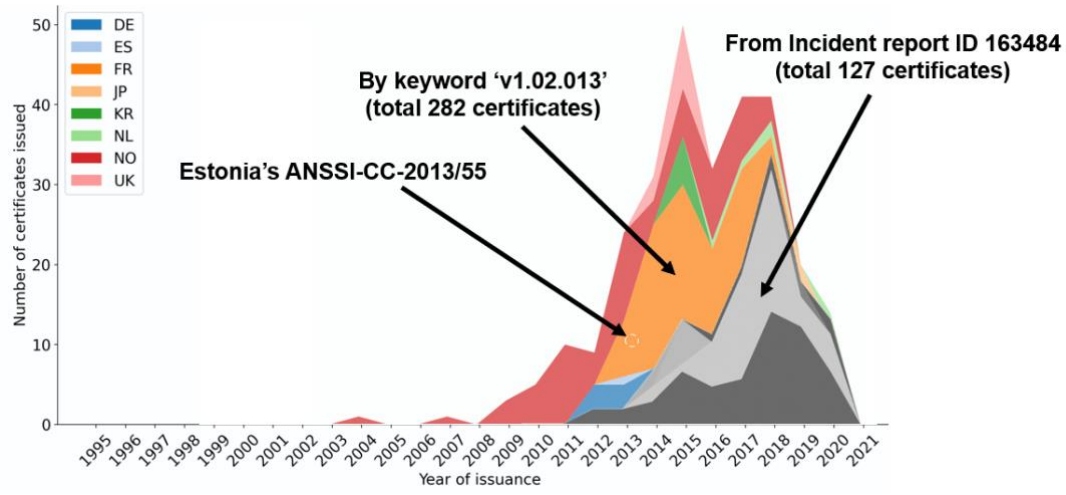

Figure 10 Visualisation of certificates relevant to a search based on a) Memo 163484 information and b) vulnerable library keyword

After the public disclosure of ROCA vulnerability, many end-users were trying to verify if their devices were also affected. While it was possible to detect vulnerable products directly from the statistical properties of generated public keys, such an option was not easily available for all systems. The published CVE description demonstrates the case of possibly incomplete or even misleading information extractable from the CVE database about a specific vulnerability. While ROCA's CVE [69] lists the exact version of the vulnerable library (RSA library 1.02.013), it mentioned only TPM modules with CPEs mostly of affected laptop platforms -- largely omitted the fact that a large majority of Infineon smartcards (including these used in electronic ID documents) chips were also vulnerable as the same library was used extensively.

The Google-powered search on the Common Criteria portal for strings 'RSALib' and '1.02.013' returns only 3 and 32 hits, respectively (despite almost one hundred base vulnerable certificates). Additionally, a user then needs to download and investigate the resulting PDF files manually.

As the exact library version was already known (in contrast to the Estonia EstID case), a simple dependency search using *--do-find-affected-keyword* v1.02.013 command automatically returns almost 300 hundred potentially vulnerable certified devices with direct or indirect connections inside the certificate dependency graph generated by seccerts tool.

8.1.2 Recommendations

The certification documents in Common Criteria and FIPS140-2/3 schemes, as well as certificate metadata, were not created with an automatic machine processing in mind. As a result, much of the analytical work subsequently employed over the certificates is limited by incomplete and noisy input data. The issues are not limited to:

- The certificates are mainly written by humans for humans with free form structure, ambiguous statements, and incomplete availability of all supporting documents.
- Missing standard unique identification of certificates and resulting ambiguous references. Significant differences among the CC schemes exist, with some using only incremental numbers while others exhibit a well-defined structured format (e.g., BSI or ANSSI). FIPS 140 uses incremental one to four digits numbers with overlapping ranges to identify both modules as well algorithms (sometimes with # symbol before), which makes it very difficult to reliably extract a map of references. Canada moved from easier to identify to harder (from Evaluation number: '383-4-138-CR' to '516 LSS'). The variation in identification makes it more prone to the

occasional omission of the version of the certificate, certification year, and alike (e.g., BSI-DSZ-CC-404-2007 vs. BSI-DSZ-CC-0404-2007).
- Typos, omissions, and inaccuracies in the certificate, including in the certificate front page with the most important information.
- Incorrect formats of the available data sources like incorrect separators in CSV files due to commas in cert names
- Vague mapping to the referenced Protection Profiles, especially when the given profile contains multiple configurations.
- Insufficient reasons provided in the rationale for maintenance certificates addressed CVEs usually completely omitted or only in non-public self-reported Impact Analysis report by Vendor.
- Lack of data for independent replication of the evaluation facility claims: Ideally, the user can independently replicate all certification steps, requires freely available tooling (ideally open source), and requires a complete log of tools and settings used.
- Ambiguous mapping of certificate to vulnerability trackers: Prepare for easy evaluation for (future) vulnerability tracking, clear referencing of used components by the certified product, clear references of vulnerability entries: CPE/CVE, anticipate future vulnerabilities found (prefill CPE).

Based on the variety of issues encountered during the certificate processing by seccerts tool, we recommend the following improvements:

- **Provide clear guidelines for certificate identification.** Currently, all certificate issuing countries have their own certificate identification format, making unambiguous referencing difficult. The certificate shall contain the certificate id in the defined metadata.
- **Always assign CPE(s) for the issued certificate**. This will remove ambiguity in the naming selected by the manufacturer and will enable a more accurate matching of certificates to a database of vulnerabilities.
- **Be more transparent in vulnerability handling**. While the certified products can include patches that prevent them from existing vulnerabilities that otherwise affect the product of such a version, the information about whether these patches are applied is not transparent. In maintenance updates, vulnerabilities are often neglected, or a generic statement that "IAR contains a rationale why these vulnerabilities do not affect the ToE" is present, while the respective report is not available to the public.
- **Enforce unified document formatting** of the certification documents, preferably in English. From some of the certificates, text cannot be easily extracted for subsequent analysis.
- **Improve data quality of both CC and FIPS websites**. As these web pages are the primary source of publicly available information, the provided inputs shall be properly formatted and authoritative. For example, the portal contains improperly formatted CSV files with duplicate rows, pdf of certain certificates not available for download, etc.
- **Create a well-defined composite structure for a certified item** for reliable detection of potentially impacted items after a vulnerability is found. For example, Security Content Automation Protocol (SCAP) [70] utilises Common Platform Enumeration (CPE) and Common Configuration Enumeration (CCE) formats.

8.2 An Example Application of Certification Using SURFACE

8.2.1 Overview

In this section we describe how to apply the SURFACE framework described in Deliverable 3.22 to the integrated circuit (chip) of the Estonian ID card. We give a practical overview how to use our methodical

approach to allow for a more transparent certification, re-certification and continuous monitoring process of a critical infrastructure component. A detailed overview of SURFACE can be read from Deliverable 3.22, however, we show the steps we employed for the chip certification also in Figure 11 to give an easier reference. SURFACE is divided into the following phases: phase 0 (reconnaissance), phase 1 (planning), phase 2 (assessments), phase 3 (generating certification elements), phase 4 (communicating the results) and phase 5 (re-certification). All of these phases are monitored by the continuous monitoring process.

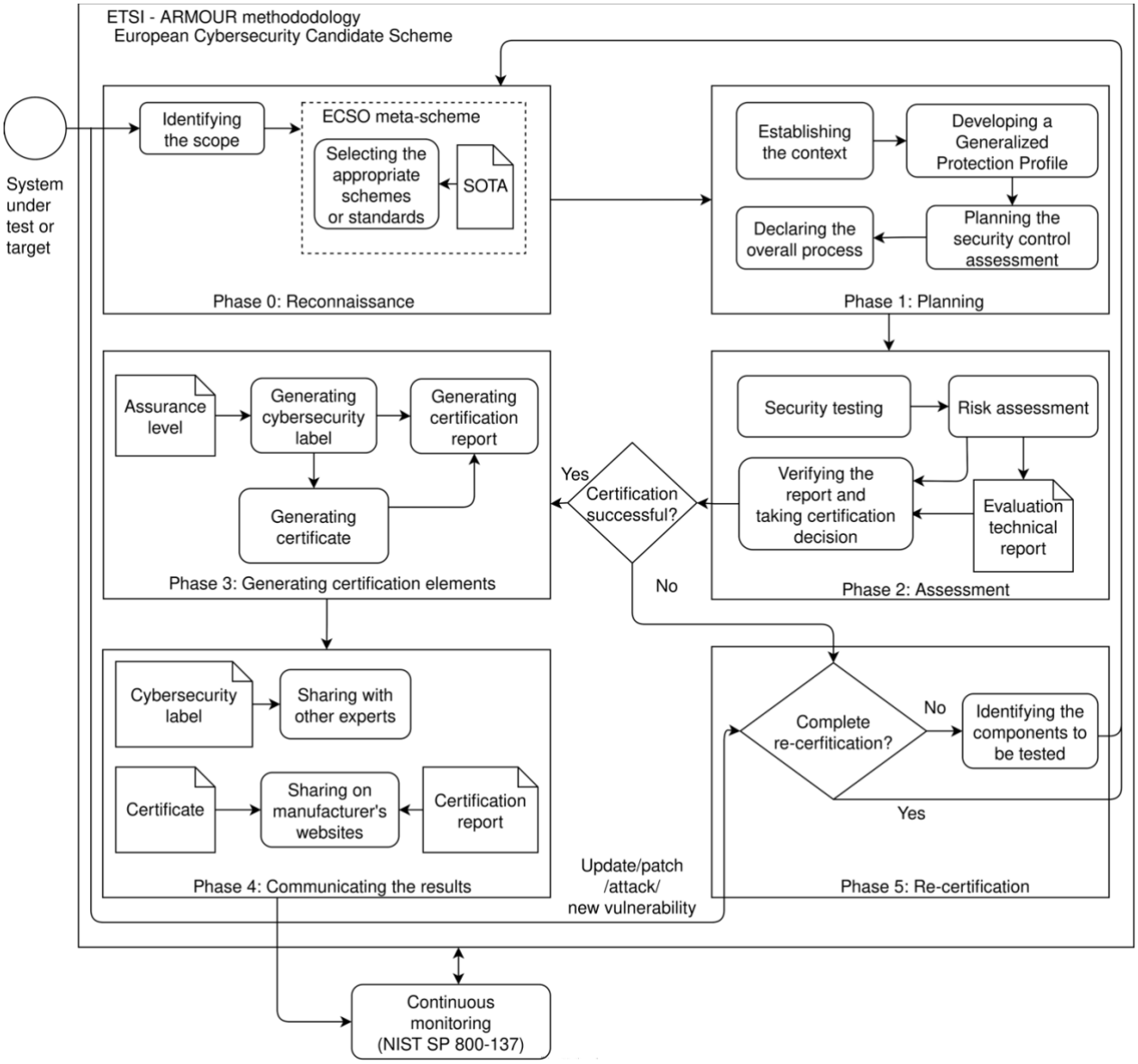

Figure 11. Overview of the certification and re-certification of the integrated circuit

8.2.1.1 Estonian ID Card

We are using the Estonian ID card chip as the basis for our examples. The Estonian ID card is a mandatory document for all citizens and residents of Estonia. It is a primary identification document and accepted throughout the European Union countries. This document can be used for authentication, authorisation (digital signatures), as a residence permit card and as a travel document. The ID cards are

issued by the Estonian Police and Border Guard Board[24] (Politsei- ja Piirivalveamet, PPA) based on the Identity Documents Act.

The ID card chips are currently manufactured IDEMIA[25]. The card manufacturer is subcontracted with the qualified trust service provider SK ID Solutions AS[26] for issuing the digital certificates to the ID card. The trust service provider is working under the legislation of eIDAS [67]. The Estonian Information System Authority[27] (Riigi Infosüsteemi Amet, RIA) is responsible for collecting information about the requirements and applications required for using the eID services.

The cryptographic mechanisms of the Estonian ID card are based on the chip configurations and the operating system involved. These cryptographic features, like key generation and key import, are implemented by the chip using the public key infrastructure application. The Identification Authentication Signature-European Citizen Card (IAS-ECC) is the Public Key Infrastructure (PKI) application used in the Estonian digital documents. It is a qualified signature creation device certified based on the following Protection Profiles [71]:

- CEN/EN 14169-2 (EN 419211-2): Device with key generation,
- CEN/EN 14169-3 (EN 419211-3): Device with key import,
- CEN/EN 14169-4 (EN 419211-4): Extension for device with key generation and trusted communication with certificate generation application,
- CEN/EN 14169-5 (EN 419211-5): Extension for device with key generation and trusted communication with signature creation application,
- CEN/EN 14169-6 (EN 419211-6): Extension for device with key import and trusted communication with signature creation application.

This IAS-ECC meets all the requirements of the CEN/TS 15480-2 [72] (European eID) documents. Thus, it can implement the security and functional use cases through various authentication mechanisms. For instance, a cardholder is authenticated using the two cryptographic keys (authentication key and digital signature key) that are present on the chip. This validation uses the Application Protocol Data Unit commands against personal data file records present on the chip [73].

8.2.1.2 Security Vulnerabilities and Attacks on the Chip

Side-channel attacks. The goal of this attack is to retrieve the cryptographic keys by identifying and exploiting the flaws from the hardware implementation of the ID card chip. The attackers usually make use of physical parameters such as electromagnetic emission, execution time, power consumption to perform side-channel attacks.

Weak RSA key generation (ROCA) (CVE-2017-15361). Initially, the Estonian ID cards used chips that were using a vulnerable software library which led to the practical factorisation attack on the commonly used key lengths (1024 and 2048 bits). This attack is possible when a remote attacker knows the public key. The attack was possible due to the usage of vulnerable chips, not because of the RSA key generation algorithm. The NIST FIPS 140-2 and CC EAL 5+ certified devices were subjected to this weak RSA key generation vulnerability [66]. The disclosure of the private key can affect the security properties such as confidentiality, authentication, integrity and non-repudiation. The products can be used in different sectors or domains, but the components can be developed using the same vulnerable hardware chip. In such cases, when the primary implementation of a product (chip) can be compromised, its impact is reflected in different areas such as ID cards, digital signing, encryption protocols.

[24] https://www.politsei.ee/en
[25] https://www.idemia.com/
[26] https://www.skidsolutions.eu/en
[27] https://www.ria.ee/en.html

8.2.2 Phase 0: Reconnaissance

Before beginning the chip certification or re-certification process, there are certain terms and conditions that are required to be accepted by the parties involved (IDEMIA and SK ID Solutions). A mutual recognition agreement (MRA) is first established between the participants. From EUCC, we adopt the terms and conditions which represent the rules and constraints for the chip certification and re-certification. Once all the conditions are declared in the MRA and it is signed by the participants involved, chip certification begins.

We will choose the following schemes for evaluating the ID card chip. These schemes are taken based on the ECSO SOTA document [56].

Common Criteria. Initially, a Protection Profile is created based on the domain and scenario of the security target. It defines a set of security functional requirements, security assurance requirements and guidelines for conducting security evaluation on security targets (a refinement of PP). Through the evaluation assurance level (EAL), CC shows the level of assurance, strictness and severity of the evaluation carried out on the target of evaluation (TOE). The latter is validated by IT Security Evaluation Facilities (ITSEF). The resulting document, the evaluation technical report (ETR) is sent to the certificate authorising scheme which decides whether to issue the CC certificate to the product. This certificate authorising scheme has recognised testing laboratories for carrying out an assessment on the target and validates ETR.

ISO/IEC 19790 Cryptographic module standards. This international standard is based on the FIPS 140-2 [74]. It is used for defining the security requirements for cryptographic modules through four security levels. The standard specifies 11 areas against which an evaluation is done. These areas are represented by statements (set of assertions). The statement defined for the module (specific to the area and security level) should be satisfied to show its conformity. The prerequisites (documentation or information) required to validate the conformity are mentioned as a set of requirements in each statement.

SURFACE allows us to combine the requirements of CC (as base scheme) and ISO/IEC 19790 using the Generalized Protection Profile (GPP). We will integrate the schemes based on the common language from the meta-scheme. We selected CC, as CC is one of the major generic security certification schemes that is recognised worldwide. ISO/IEC 19790 is integrated with CC because of the nature of the ID card. SURFACE provides a higher level of assurance than using a single evaluation scheme or standard.

The expert group (EG) also gathers necessary technical and non-technical information about the system under test (SUT). For our example, the EG is composed of the authors. The EG listed a set of threats or vulnerabilities based on the described attacks and features of the chip. The EG also considered certain vulnerabilities related to the chip functionalities from the NIST Vulnerability Database. Table 1 represents the mapping of selected threats to the security properties based on the features of the chip.

Threats	Associated Security Property or Vulnerability	Source of mapping
When the keys are easily factorisable, computing the private keys through timing side channels	Insecure cryptography	Literature
Cryptographic suite – vulnerable algorithm, improper implementation	Lack of authentication, Lack of confidentiality, Lack of integrity	Literature
Using valid ID card but invalid or outdated certificates	Lack of authentication	Literature

Retrieval of keys from memory through side channel attacks	Lack of authorisation	NIST Vulnerability Database
Spoofing due to the usage of weak pseudorandom number generator	Lack of authentication	NIST Vulnerability Database

Table 1:Selected threats and their security properties

Information gathering is required for screening the certification schemes or standards and threats that are associated with the chip. Once the EG has sufficient knowledge about the chip, they can proceed further. The EG mapped the threats to the associated security properties or vulnerabilities. These vulnerabilities help in creating a Generalized Protection Profile (GPP) and are used in the testing process to verify the conformity of the SUT.

The EG used the guidelines from [9] for the scheme selection from the ECSO State of The Art Syllabus (SOTA) [56]. Initially, the EG shortlisted certification schemes and standards for the chip based on the schemes and standards available for ICT product evaluation. Further filtration is done based on the functionalities involved in the chip. This kind of selection is in accordance with the CSA Article 54 [10] and the conditions are specified in the MRA. Note that vendors are allowed to decide whether their product should be certified against national or international schemes or standards.

As discussed in Deliverable 3.22, during the planning phase, the EG integrates the schemes based on common language from the ECSO meta-scheme. The EG is also responsible for generating the rules of engagement (ROE) based on the template from NIST SP 800-115 [75], containing information like the point of contact, constraints, and scope. The ROE are developed for the IT Security Evaluation Facilities (ITSEF) who has to follow these rules during the assessment. The EG also declares the privacy policies that are to be maintained by ITSEF.

8.2.3 Phase 1: Planning

8.2.3.1 Establishing the Context

In the planning phase, the EG defines the scope and purpose of the target. For our example the EG analyses the chip requirements and functionalities in terms of appropriate security properties, business processes, working environment, related laws. The EG derives different profiles with unique names. These profiles represent different features of the chip along with acceptable risk levels specific to appropriate vulnerabilities. These acceptable risk levels are generated based on the business and environmental conditions. Also, these acceptable risk levels are compared with the actual risk levels to make a decision.

SURFACE allows the chip to be certified either against a specific Protection Profile (PP) or the EG can create its own GPP based on the reconnaissance phase, context establishment and different existing PPs. For instance, when only a specific component of the chip has to be certified, the EG specifies the particular PP against which the chip component gets certified. When the entire chip requires certification, the EG can create a GPP based on Common Criteria PP for the security integrated circuit (IC) platform [76] and Common Criteria PPs for secure signature creation device [77]. This GPP represents the problem definition, objectives that satisfy the requirements of both CC and ISO/IEC 19790. It is also required to specify the constraints (if any) related to the chip.

As mentioned in EUCC [9] and CC [82], the developed GPP is evaluated by an accredited ITSEF. If the evaluation is successful, a unique ID will be provided to the evaluated GPP and a certificate can be generated. The GPP is allowed to undergo any relevant updates or changes based on the chip requirements. The GPP certificates can be added as a subset of the ID card chip certificate and it is not mandatory to define under the supplementary cybersecurity information [9].

8.2.3.2 Assessment Planning

The success of certification is determined based on the assessment results against the threats from Table 1. The EG plans the assessment activities, prioritises the tests for the vulnerabilities based on the acceptable risk levels, selects the testing techniques, selects the risk assessment approach, and develops an overall certification plan or process.

As the testing techniques, the EG chose model-based testing and penetration testing. The chip manufacturer decides whether ITSEF has to carry out black-box testing, grey-box testing or white-box testing. For the risk assessment approach, the EG chose the Common Vulnerability Scoring System to identify the risk levels for the exploitable vulnerabilities. As we are aiming for accredited assessment and we do not consider self-assessment of conformity sufficient for this purpose, the testing and risk assessment has to be done by an accredited third party (ITSEF). Finally, an overall plan for the chip certification is created based on Phase 0, context establishment and assessment decisions. This plan is in compliance with the responsibilities of CC and ISO/IEC 19790. The detailed explanation of the chip assessments and their responsibilities are further discussed in Section 8.2.4 (Phase 2).

8.2.3.3 Certification Process Development

Before beginning the evaluation of the chip, all the mandatory supporting elements and guidance supporting documents are provided. These documents help the chip evaluator to gain more knowledge on the chip functionalities, its requirements and also guides on carrying out the chip evaluation. Where applicable, the evaluator must be supplied with all the necessary and appropriate information during the evaluation of the chip. The supporting documents that are used by the evaluator during the certification and re-certification processes are included in the evaluation technical report (ETR) and the certification report [9]. IDEMIA is certified with Level 1 and Level 2 of ISO/IEC 30107-3 [78]. SK ID Solutions is responsible for certificate management and is ISO/IEC 27001 certified [79].

We have defined the following overall chip evaluation process based on the CC certification scheme [56] and meta-scheme [58].

1. A GPP is created based on the chip context which is in compliance with the CC and ISO/IEC 19790. Note that if a new GPP cannot be declared, existing PPs can be used.
2. The developed GPP is provided with the acceptable risk levels specific to the vulnerability.
3. The developed GPP is approved and certified by an accredited testing laboratory.
4. The selected vulnerabilities, security requirements to be achieved, and other required documentation are given as input for the security testing process.
5. The recognized evaluation laboratory, ITSEF (tester or evaluator) reads all the supporting documents like technical documentation, rules of engagement. ITSEF proceeds by security testing the chip against the chosen vulnerabilities. A vulnerability scan can be carried out by the tester to discover any new vulnerabilities (tools can be chosen by the tester or vendor). If a new vulnerability is found during this scan, the vulnerability is added to the list of chosen vulnerabilities.
6. ITSEF carries out the tests and provides the results to the risk assessment process to generate risk levels for the vulnerabilities found. Then the tester generates evaluation technical report (ETR).
7. The certificate authorising scheme[28] is responsible for verifying the ETR and may approve or revoke the certificate for the chip based on the results.
8. The certification report is generated by the certificate issuer based on the ETR.
9. If the certificate has been approved, cybersecurity label is generated using the QR code representing the level of security properties. The cybersecurity label is communicated with other

[28] https://www.commoncriteriaportal.org/ccra/schemes/?CFID=54353509CFTOKEN=f145320dd3e9180a-126069DE-155D-014B-516CDDC16529A411

researchers and experts. If the certificate has been revoked, results are communicated and re-certification process shall proceed. Re-certification is discussed in Section 8.2.7.

8.2.4 Phase 2: Assessment

In this phase, ITSEF or the tester is responsible for executing the testing and risk analysis process for the chip evaluation. They are provided with all the mandatory documents along with the rules of engagement. The related vulnerabilities along with the acceptable risk levels of the chip are provided as inputs to the testing process. CC provides a set of responsibilities which have to be carried out but not the procedure or steps on how to accomplish them. Sections 3 and 4 give an overview of different testing and risk assessment methods which can be used to choose the best approach for carrying out the evaluation.

Figure **12** gives an overview of the assessment phase of chip certification. In this figure, MBT is shorthand for model-based testing and PT is penetration testing.

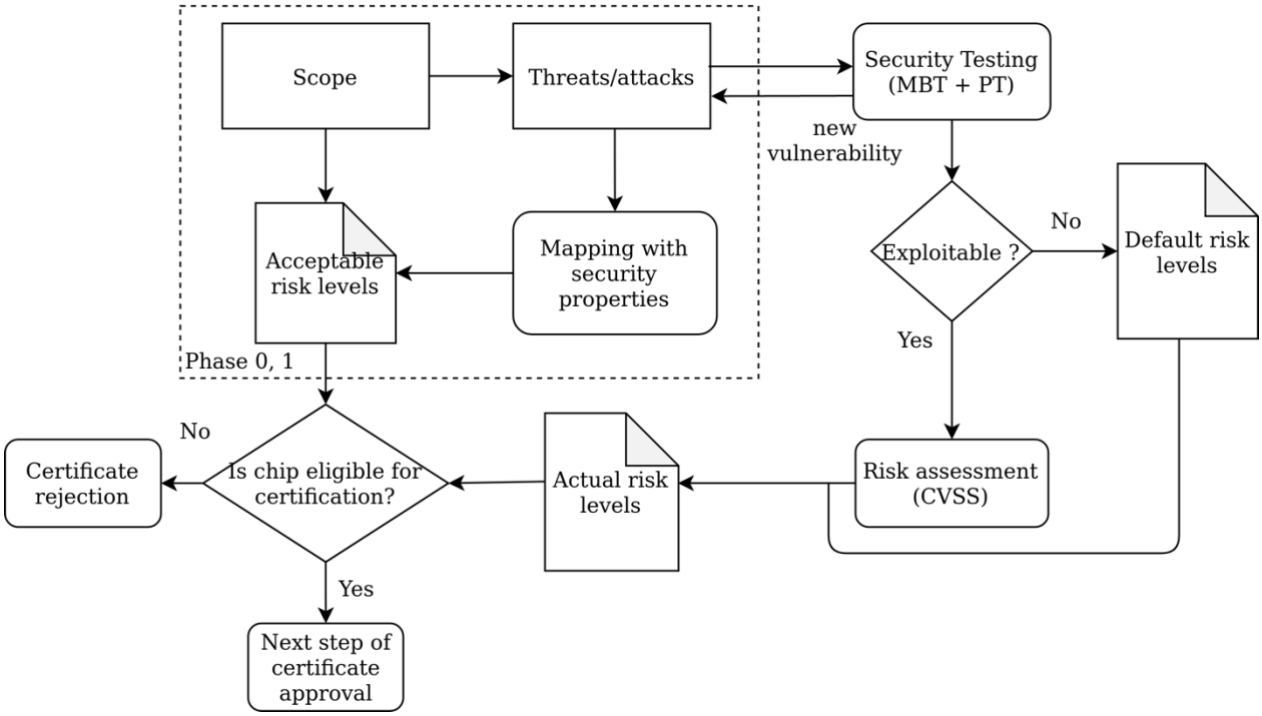

Figure 12. Assessment phase for the chip

8.2.4.1 Model-Based Penetration Testing

Test case generation. ITSEF uses model-based testing to generate the test cases for the penetration testing scenarios using the CertifyIt tool [27] based on the selected vulnerabilities. Though the test cases are generated automatically, some processes like model design, test specification and adapter implementation are done manually by ITSEF. However, the generated designs can be reused (or with minor modifications) for future tests (re-certification). In that case, the implemented adapter can be extended if more tests need to be executed on the target.

Test execution. To verify whether the selected vulnerabilities are exploitable on the security target, penetration testing is used. We chose penetration testing to depict and get an idea about how an actual attack can be carried out and the impact it can cause. As mentioned previously, the chip manufacturer is responsible for specifying the type of penetration testing that should be carried out on the chip. Mostly penetration testing is a manual process with the help of some automated tools. Hence ITSEF makes use of the technical guidance from Penetration Testing Execution Standard (PTES) documentation [80] for

the test execution step. PTES provides a common language for carrying out penetration testing and reporting all its results. We assume that ITSEF carries out penetration testing on the test cases generated from the test case generation step based on PTES guidelines. Then ITSEF reports all the findings as a technical report based on PTES for future use. This technical report is given as input to the risk assessment process.

ITSEF are allowed to use any appropriate automated tools or the tools approved by the ID card chip manufacturer. In addition to testing against selected vulnerabilities, ITSEF can either manually or using a vulnerability scanner, identify new or zero-day vulnerabilities. If any new vulnerabilities are found during the penetration testing process, a copy of that vulnerability is sent to Phase 1 as shown in Figure 12 so that it can be mapped to the appropriate security property according to its context or domain. Test cases are generated for this new vulnerability under test case generation. ITSEF reports the finding related to this new vulnerability in a technical report and report is given as input to the risk assessment process. Note that other testing methods like fuzz testing or code-based testing can also be a part of the penetration testing based on the type of ICT product.

8.2.4.2 Risk Assessment

The CC process does not include risk assessment, however the SURFACE framework does. The exploitable vulnerabilities found during testing are given as input to the risk analysis process so the actual risk level can be determined. We make use of the Common Vulnerability Scoring System (CVSS) to compute the risk level. Table 2 shows the risk levels based on CVSS v3.1 [44].

CVSS score	Risk level
0.0	None
0.1-3.9	Low
4.0-6.9	Medium
7.0-8.9	High
9.0-10.0	Critical

Table 2: Risk levels based on CVSS v3.1

The risk score is calculated based on the CVSS formula for every profile related to the exploitable vulnerability based on the metrics (base, temporal and environmental). Finally, the estimated score is mapped to the risk levels shown in Table 2. SURFACE allows ITSEF to use any accredited risk assessment tool (certified against any international standard) to carry out the risk assessment based on CVSS v3.1 on the exploitable vulnerabilities where applicable.

The results of the testing and risk assessment of the chip are compiled into an evaluation technical report (ETR). The ETR should contain information about the type of penetration testing used in the chip evaluation along with valid evidence to prove the assurance level on the chip. This ETR can be reused or referred to during future testing. The ETR and other sensitive information of chip assessment (results of risk assessment, penetration testing) must be shared only with the chip manufacturer or manufacturer approved person.

8.2.4.3 Certification Decision

Based on the outcomes of the testing and risk assessment, the certificate authorising scheme determines whether the certification approval can proceed. The actual state of the baseline security of the chip is compared with the expected state. The assessed risk levels are compared with the acceptable risk levels generated by the EG in the planning phase. A profile is considered fulfilled if the acceptable risk level matches the actual risk level.

When all the profiles are fulfilled, the chip is considered to be eligible for certification and proceeds to the next phase. In addition to the profile fulfilment, evidence for performed evaluation (ETR) must be provided to the certificate authorising scheme [9]. When a profile is not fulfilled, the identified threats should be mitigated and the profile is then prioritised for re-certification based on the risk level. Table 3 represents the certificate decisions based on the assessment results and the evidence provided.

Assessment result	Decision
The ID card chip meets the requirement criteria	Issue the certificate
The certificate of the ID card chip expired, no updates or modifications or an attack was discovered and the new assessments were successful (upon vendor's request)	Continue the certificate and extend the validity
The certified chip components had updates or modifications or an attack was discovered (certificate may or may not have expired) and the new assessments were successful	Renew the certificate with extended validity
The certificate of the ID card chip expired, no updates or modifications or attack was discovered and the new assessments were not successful (upon vendor's request)	Suspend the certificate validity. Proceed with re-certification after remedial measures
The certificate of the ID card chip expired and vendor did not request certificate maintenance	Archive the certificate
The certified chip components had updates or modifications or an attack was discovered (certificate may or may not have expired) and the new assessments were not successful	Suspend the certificate and proceed with re-certification after remedial measures
The necessary assessments were not successful for the same chip version, but works with reduced assurance level or scope	Continue or renew the certificate with reduced assurance level or scope and extend its validity
The assessments were not successful and no possible actions can be performed	Do not issue certificate or withdraw the certificate
Improper certificate or cybersecurity label usage	Suspend the certificate and respective authority (PPA or ID card manufacturer) should make corrective measures
Proper remedial or corrective measures are not taken within the given time	Do not issue certificate or withdraw the certificate

Table 3: Certificate decisions based on the assessment results

8.2.5 Phase 3: Generating Certification Elements

The penetration testing type determines the assurance level of the methodology. This assurance level is included in the certificate and cybersecurity label of the certified chip. The certification report must also contain the assurance level with detailed information. Table 4 represents the assurance levels.

Type of penetration testing	Assurance level	Assessment type
Black-box penetration testing	Base	ITSEF

Gray-box penetration testing	Substantial	ITSEF
White-box penetration testing	High	ITSEF

Table 4: Assurance level with respect to penetration testing type

The created certification report contains all the information about the chip certification process. The certificate issuer creates the report based on the evaluation technical report (ETR). The report can be published on the CC portal or the manufacturer's website. SURFACE encourages the use of a structured certification report to allow for an easy overview and comparison of the certificates. A reference to the certification report is added to the certificate.

The cybersecurity label for the ID card chip should be generated only when the certification is completed successfully. It is valid only for a limited period of time determined by the certification validity. If the assessment criteria are not fulfilled, use of the cybersecurity label on the chip is prohibited [9]. Based on the ARMOUR methodology, the label contains the following:

1. the QR code with a link to the generated certificate,
2. the security properties and its level present on the chip,
3. the assurance level: basic or substantial or high,
4. validity information.

The chip manufacturer generates a multi-dimensional label to represent the level of different security properties. Figure 13: Example cybersecurity label for the ID card chip gives an example of a cybersecurity label for the ID card chip. As it is not mandatory to display the label on the certified product, the manufacturer can decide whether to add the label on the certified product.

Figure 13: Example cybersecurity label for the ID card chip

8.2.6 Phase 4: Communicating the Results

In this phase, we can communicate the chip evaluation results with experts or researchers through the cybersecurity label. The certificates generated for the certified chips are valid for a maximum of five years from the date of certificate issuance [9]. This initial period of validity can be extended if the certified ID card chip still meets its required security baselines. On the other hand, if any of the adverse conditions in Table 3 occurred before the expiration of the chip certificate, the validity ends.

All the information related to the certified chip such as the certification report, the certificate, and the cybersecurity label can be made available on the chip manufacturer website, CC portal, or any other website in accordance with the CSA Article 55 and Article 50 [10]. Also, the certificate issuer is responsible for establishing the guidelines or rules on how to deliver and publish the certification data of the chip.

The published information is available for five years after the expiration date of the chip certificate. The availability time may change if the chip undergoes re-certification and information is made available for five years from the newly assigned expiration date.

8.2.7 Phase 5: Re-certification

Incremental Certification. Generally, the re-certification of the chip or any product has a high cost and is time-consuming. With the help of continuous monitoring, we can identify the changes and re-certify only the necessary parts if there is a minor change or update. If any major update or change or identification of new threat or vulnerability occurred, then re-certification of the entire chip is necessary.

A safety case[29] (SC) represents proof or evidence ensuring that a system is safe to use in the given environment through a set of organised arguments. The EG is required to define the modular SC for the chip enabling isolation between modules (with agreed interfaces) and reuse. By using modular SC, SURFACE allows certifying only the specific component that requires re-certification instead of re-certifying the whole chip (unless required otherwise). The EG can take the following steps throughout the phases to allow for modular and incremental certification.

Step 1. During context establishment (Phase 1), the EG analyses the chip functionalities and its life-cycle. This helps to understanding the changes carried out on the chip and in developing the SC.

Step 2. Based on the information from Step1, the EG identifies why, how and what has been changed. Then the EG compares the change scenario on the chip with various scenarios. In case a new vulnerability was detected, the EG should consider all the profiles that are related to the new vulnerability.

Step 3. If the change is major, then the chip undergoes full re-certification. Otherwise, the EG proceeds with the following steps.

Step 4. The EG defines the SC architecture for the chip. The SC modules are derived by the EG based on the level of cohesion and coupling, module interfaces and level of abstraction (information hiding). The EG identifies dependencies among each module and with the environment through dependency-guarantee relationships (DGR). DGRs can be represented using software elements involved in the chip design. A dependency-guarantee contract (DGC) defines the relationship between the software elements.

Step 5. A safety argument (SA) is generated by the EG for each SC module and mostly uses appropriate DGRs to show that the dependency of one module is supported by another module. Now the EG links the SA modules to represent the entire system of the chip processes. These SA modules are integrated

[29] https://www.amsderisc.com/wp-content/uploads/2013/01/IAWG-mod-cert-briefing-v5.pdf

through the DGC defined in the SC. The advantage of using this SC contract is that modules are not linked directly. Here a module (which requires support) is linked to the SC contract which then identifies the appropriate module that is ready to support that dependency. By this, changes in the module do not reflect on the indirectly linked modules. The EG integrates all SC modules within the SC by mapping all the dependencies generated for each module.

Step 6. With the help of the SC, the EG has to identify all the profiles that are related to the changes that have been detected. Where applicable, new profiles can be derived based on the context.

Step 7. The EG assesses the change through impact and acceptable risk levels on that profile for all applicable vulnerabilities. For newly identified vulnerabilities, acceptable risk levels are generated by the EG for the profiles.

Step 8. All the requirements from step 1-7 are accomplished and given as input to the planning phase to update the Generalised Protection Profile and the security target. Compliance is verified against CC requirements. All the previous assessment reports and required documents can be shared with ITSEF under the EUCC for assessing the security strength of the modified chip. Then ITSEF carries out the assessment and provides proper evidence. Based on the evidence, the certificate authorising scheme decides whether to provide a certificate to the chip. Finally, the results are shared and a common unified report is generated.

Note that if more than one change scenario occurred, scenarios are prioritised based on the significance of the scenario or impact that can be caused by the vulnerability if exploited.

8.3 Continuous Monitoring

Continuous monitoring (CM) is required throughout the certification of the chip and even after that. The fundamental goal of CM is to support risk management and re-certification. Also, through CM we can enable proper maintenance and verify the certificate validity of the chip periodically. We can use CM to verify whether the certification or re-certification of the chip complies with the guidelines of the EUCC.

Step 1. An Information Security Continuous Monitoring (ISCM) strategy is defined. Information about the chip is provided for the strategy. This information includes details about assets, previous and up-to-date vulnerabilities, threats, acceptable risk levels, functionalities, associated impact, the EG, ITSEF, available certification schemes or standards, ROE, GPP, the MRA.

Step 2. The metrics and set the frequencies for monitoring and reporting are determined. The metrics can be derived from assessment result status reports, predefined vulnerabilities (Table 1) or other security information gathered by the EG in Phases 0 and 1. A technical architecture is developed. This architecture defines how the information from Step 1 is collected, how that information is stored, how the information is analysed and accessed for response and how the status reports are generated. This architecture helps in understanding the overall workflow of monitoring and its interoperability.

Step 3. The technical architecture is implemented and the monitoring is initiated. Assessments are conducted and related information are collected and stored. The frequency for the generation of a status report about the assessment is set.

Step 4. The monitoring results, status reports and other collected information are analysed and verified by the EG manually at periodic intervals. If a component requires mitigation actions, the EG is responsible for verifying whether appropriate actions have been carried out. The EG reports all the findings in a document after analysing and the report is stored in the repository.

Step 5. The vendor decides how to handle all the findings made by the EG. When any chip profile is not fulfilled, appropriate measures are taken by the mitigation team to mitigate the corresponding exploitable vulnerability. Also, if any issues are detected on the certified chip, then existing processes are put on hold until the chip is subjected to re-certification. Status reports should be generated when the appropriate response decisions are taken.

Step 6. Based on the findings and the chip certification requirements and enabled monitoring features, the ISCM strategy is refined in terms of visibility of information, frequency of monitoring or reporting and metric determination. When any deviations are found, appropriate decisions or actions must be taken based on the MRA. Once the chip manufacturer carries out all the updates or remediation, the notification of ITSEF and the initiation of the re-certification of the chip can be automated. Then the approved ITSEF is notified to proceed with assessment (Phase 2).

9 Conclusion

This deliverable gives an overview of different certification schemes, testing and risk assessment methods. We talk about the goals of cybersecurity certification, and identify and discuss challenges that the field faces. Based on the gathered information, we conclude that there is a need to make the certification process more approachable and affordable, the results more visible and comparable.

We propose a solution in the form of a virtual certification centre, which if used together with the SURFACE certification framework from Deliverable 3.22 *Validation and Certification Methodology* will alleviate most of the identified challenges, but especially the lack of transparency and lack of communicability. The proposed structured and machine-readable evaluation reports and dependency graphs help visualise and communicate the certification results while also simplifying the visibility of dependencies in case vulnerabilities are found in technologies upon which that the product relies.

We implemented and continue to operate the virtual certification centre as virtual overlay over the existing security certification schemes. This means that is not a new certification scheme, but rather allows to use the manufacturer's or vendor's favourite existing scheme or combination of schemes as the basis for certification, giving flexibility, and widening the market and uptake. The centre is available at https://seccerts.org.

The centre connects certified items with certification schemes and vulnerability databases. This helps the users of certified products to assess the target item before purchasing and obtain faster notification if vulnerabilities are discovered. Once the centre gains traction and is more widely used, we believe that the information in the virtual centre will also influence the transparency of the underlying certification schemes.

Bibliography

[1] CCRA, "Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model," 2017.

[2] Common Criteria, "Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security," [Online] https://www.commoncriteriaportal.org/files/operatingprocedures/cc-recarrange.pdf, 2014.

[3] C. Zhou and S. Ramacciotti, "Common Criteria: Its Limitations and Advice on Improvement," *ISSA J.*, 2011.

[4] S. P. Kaluvuri, M. Bezzi and Y. Roudier, "A Quantitative Analysis of Common Criteria Certification Practice," *Trust, Privacy, and Security in Digital Business*, vol. 8647, pp. 132-143, 2014.

[5] F. Keblawi and D. Sullivan, "Applying the common criteria in systems engineering," *IEEE Secur. Priv. Mag.*, vol. 4, no. 2, pp. 50-55, 2006.

[6] CESG, "The Commercial Product Assurance (CPA) build standard," [Online] https://www.nccgroup.trust/uk/our-services/cyber-security/compliance-and-accreditations/cpa-and-cc/, 2015.

[7] National Cybersecurity Center of the United Kingdom, "Foundation Grade explained," [Online]. https://www.ncsc.gov.uk/articles/foundation-grade-explained, 2017.

[8] Underwriters Laboratories, "UL 2900 Standards Process," [Online]. https://industries.ul.com/cybersecurity/ul-2900-standards-process.

[9] ENISA, "Cybersecurity Certification: EUCC Candidate Scheme," [Online] https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme, 2020.

[10] Cybersecurity Act, "Regulation (EU) 2019/881 Of The European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 52," [Online]. https://eur-lex.europa.eu/eli/reg/2019/881/oj, 2019.

[11] ANSSI, "Certification de sécurité de premier niveau (CSPN)," [Online]. https://www.ssi.gouv.fr/administration/produits-certifies/cspn/, 2008.

[12] CryptoExperts, "Certification de securite de premier niveau," [Online]. https://www.cryptoexperts.com/services/cspn/.

[13] G. Baldini, G. Giannopoulos and A. Lazari, "Annex 8: JRC Analysis and recommendations for a European certification and labelling framework for cybersecurity in Europe," European Commission, 2017.

[14] Aeronautical Radio Inc, "ARINC 651. Design Guidance for Integrated Modular Avionics," 1991.

[15] Aeronautical Radio Inc, "ARINC 653, Avionics Application Software Standard Interface," 1997.

[16] M. Adnan, *Exact Worst-Case Communication Delay Analysis of AFDX Network*, Thèse de doctorat, Institut National Polytechnique de Toulouse, 2013.

[17] M. Grenier, L. Havet and N. Navet, "Pushing the limits of CAN-scheduling frames with offsets provides a major performance boost," in *4th European Congress on Embedded Real Time Software (ERTS 2008)*, 2008.

[18] N. Badache, K. Jaffrès-Runser, J.-L. Scharbarg and C. Fraboul, "Managing temporal allocation in Integrated Modular Avionics," in *Proceedings of IEEE International Conference on Emerging Technology & Factory Automation (ETFA 2014)*, Barcelona, Spain, 2014.

[19] N. Badache, *Allocation temporelle de systèmes avioniques modulaires embarqués*, Thèse de doctorat, Institut National Polytechnique de Toulouse, 2016.

[20] Q. Wang, K. Jaffrès-Runser, Y. Xu and J.-L. Scharbarg, "A certifiable resource allocation for real-time multi-hop 6TiSCH wireless networks," in *13th IEEE International Workshop on Factory Communication Systems (WFCS17)*, Trondheim, Norway, 2017.

[21] CNSSI, "CNSSI No. 4009: Committee on National Security Systems (CNSS) Glossary," [Online]. https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf, 2015.

[22] F. Bouquet, C. Grandpierre, B. Legeard, F. Peureux, N. Vacelet and M. Utting, "A subset of precise UML for model-based testing," in *3rd international workshop on Advances in model-based testing (A-MOST 2007)*, London, United Kingdom, 2007.

[23] M. Felderer, B. Agreiter, P. Zech and R. Breu, "A Classification for Model-Based Security Testing," in *VALID 2011, The Third International Conference on Advances in System Testing and Validation Lifecycle*, 2011.

[24] J. Cabot and M. Gogolla, "Object Constraint Language (OCL): A Definitive Guide," in *12th international conference on Formal Methods for the Design of Computer, Communication, and Software Systems: formal methods for model-driven engineering*, 2017.

[25] A. Cretin, B. Legeard, F. Peureux and A. Vernotte, "Increasing the Resilience of ATC systems against False Data Injection Attacks using DSL-based Testing," in *Doctoral Symposium ICRAT*, 2018.

[26] W. Li, F. Le Gall and N. Spaseski, "A Survey on Model-Based Testing Tools for Test Case Generation," *Tools and Methods of Program Analysis*, vol. 779, pp. 77-89, 2018.

[27] B. Legeard and A. Bouzy, "Smartesting CertifyIt: Model-Based Testing for Enterprise IT," in *IEEE Sixth International Conference on Software Testing, Verification and Validation*, Luxembourg, Luxembourg, 2013.

[28] S. Yoo und M. Harman, „Regression testing minimization, selection and prioritization: a survey,“ *Softw. Test. Verification Reliab.*, Bd. 22, Nr. 2, pp. 67-120, 2012.

[29] M. Felderer and E. Fourneret, “A systematic classification of security regression testing approaches,” *Int. J. Softw. Tools Technol. Transf.*, vol. 17, no. 3, pp. 305-319, 2015.

[30] E. Fourneret, F. Bouquet, F. Dadeau and S. Debricon, “Selective Test Generation Method for Evolving Critical Systems,” in *IEEE Fourth International Conference on Software Testing, Verification and Validation Workshops*, Berlin, Germany, 2011.

[31] L. Cseppento and Z. Micskei, “Evaluating code-based test input generator tools,” *Softw. Test. Verification Reliab.*, vol. 27, no. 6, pp. 22-29, 2017.

[32] B. Chess and J. West, Secure programming with static analysis, Gary McGraw, 2007.

[33] N. Ayewah, D. Hovemeyer, J. D. Morgenthaler, J. Penix and W. Pugh, “Using Static Analysis to Find Bugs,” *IEEE Softw.*, vol. 25, no. 5, pp. 22-29, 2008.

[34] M. Bishop, “About Penetration Testing,” *IEEE Secur. Priv. Mag.*, vol. 5, no. 6, pp. 84-87, 2007.

[35] J. Bau, E. Bursztein, D. Gupta and J. Mitchell, “State of the Art: Automated Black-Box Web Application Vulnerability Testing,” in *IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 2010.

[36] ISECOM, “The Open Source Security Testing Methodology Manual (OSSTMMv3),” 2010.

[37] C. Chen, B. Cui, J. Ma, R. Wu, J. Guo and W. Liu, “A systematic review of fuzzing techniques,” *Comput. Secur.*, vol. 75, pp. 118-137, 2018.

[38] C. Miller and Z. Peterson, “Analysis of mutation and generation-based fuzzing,” 2007.

[39] W. Krenn, R. Schlick, S. Tiran, B. Aichernig, E. Jobstl and H. Brandl, “MoMut - UML Model-Based Mutation Testing for UML,” in *IEEE 8th International Conference on Software Testing, Verification and Validation (ICST)*, Graz, Austria, 2015.

[40] F. Duchene, “Detection of Web Vulnerabilities via Model Inference assisted Evolutionary Fuzzing,” Grenoble University, 2014.

[41] MITRE, “CWE - Common Weakness Scoring System (CWSS),” [Online]. https://cwe.mitre.org/cwss/cwss_v1.0.1.html, 2014.

[42] J. R. C. Nurse, S. Creese and D. D. Roure, “Security Risk Assessment in Internet of Things System,” *IEEE Comput. Soc. IT Pro*, vol. 19, no. 5, pp. 20-26, 2017.

[43] MITRE, “Common Weakness Risk Analysis Framework (CWRAF),” [Online]. https://cwe.mitre.org/cwraf/.

[44] FIRST, "Common Vulnerability Score System (CVSS) v3.1.," [Online]. https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf, 2015.

[45] Microsoft, "DREAD scheme," [Online]. https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)#dread, 2010.

[46] OpenStack, "Security/OSSA-Metrics," Online]. https://wiki.openstack.org/wiki/Security/OSSA-Metrics#Calibration.

[47] A. B. Garcia, R. F. Babiceanu and R. Seker, "Trustworthiness requirements and models for aviation and aerospace systems," in *Integrated Communications, Navigation, Surveillance Conference (ICNS)*, Herndon, VA, 2018.

[48] NCCGroup, "Threat prioritisation: DREAD is dead, baby?," [Online]. https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2016/march/threat-prioritisation-dread-is-dead-baby/, 2016.

[49] OWASP, "OWASP Application Security Verification Standard (ASVS) Project," Online] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[50] R. M. R. K, "Security risk assessment of Geospatial Weather Information System (GWIS) using integrated CVSS approach," *Int. J. Adv. Comput. Sci. Appl.,* vol. 1, no. 3, 2010.

[51] VERACODE, "VerAfied Methodology," [Online]. https://help.veracode.com/reader/kJC1iOtXp8N~rCtV8P9jhw/UQa~oUCwYhluVREDo4480g.

[52] VERACODE, "Nextcloud, Veracode Detailed Report," [Online]. https://nextcloud.com/wp-content/themes/next/assets/files/veracode_report.pdf?x16328, 2016.

[53] CENZIC, "HARM Score," [Online]. http://doc.cenzic.com/sadoc9x14ba847/harm.htm.

[54] J. Eichler and D. Angermeier, "Modular Risk Assessment for the Development of Secure Automotive Systems, VDI/VW-Gemeinschaftstagung Automotive Security," VDI-Berich, 2015.

[55] ETSI, "ETSI TS 102 165-1 Methods and protocols; Part 1: Method and proforma for Threat, Vulnerability, Risk Analysis (TVRA)," 2017.

[56] ECSO, "State of the Art Syllabus v2," [Online] http://www.ecs-org.eu/documents/uploads/updated-sota.pdf, 2017.

[57] H. Baars, R. Lassche and H. Pille, "Smart grid security certification in Europe. Challenges and recommendations," ENISA, 2014.

[58] ECSO, "A Meta-Scheme Approach v1.0," [Online] http://www.ecs-org.eu/documents/uploads/european-cyber-security-certification-a-meta-scheme-approach.pdf, 2017.

[59] P. Radanliev, D. C. De Roure, J. R. C. Nurse, R. M. Montalvo und P. Burnap, „Standardisation of cyber risk impact assessment for the Internet of Things (IoT)," *IJSART,* Bd. 5, Nr. 11, pp. 9-12, 2019.

[60] S. Murdoch, M. Bond and R. J. Anderson, "How Certification Systems Fail: Lessons from the Ware Report," *IEEE Secur. Priv. Mag.*, vol. 10, no. 6, pp. 1-1, 2012.

[61] M. Bartoletti, P. Degano and G. L. Ferrari, "Security Issues in Service Composition," *Formal Methods for Open Object-Based Distributed Systems*, vol. 4037, pp. 1-16, 2006.

[62] RASEN project, "D3.2.3. Techniques for Compositional Test-Based Security Risk Assessment v.3," [Online] http://www.rasenproject.eu/downloads/985/.

[63] AIOTI, "Report on Workshop on Security and Privacy in the Hyper-Connected World," 2016.

[64] J. Hubner and M. Lastovka, "BOSCH Political Viewpoint. Security in IoT.," 2017.

[65] J. Hearn, "Does the Common Criteria paradigm have a future?," *IEEE Secur. Priv. Mag.*, vol. 2, no. 1, pp. 64-65, 2004.

[66] M. Nemec, M. Sys, P. Svenda, D. Klinec and V. Matyas, "The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli," in *ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA, 2017.

[67] European Union, *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS)*, https://eur-lex.europa.eu/eli/reg/2014/910/oj, 2014.

[68] "eIDAS incident report memo ID-163484, Austria," [Online]. https://cybersec.ee/storage/Incident-report-ID-163484-Austria.pdf, 2017.

[69] NIST, „NIST National Vulnerability Database, CVE-2017-15361 vulnerability detail," [Online]. https://nvd.nist.gov/vuln/detail/CVE-2017-15361.

[70] D. Waltermire, S. Quinn, H. Booth, K. Scarfone and D. Prisaca, "Security Content Automation Protocol v1.3, NIST Special Publication 800-126 revision 3," [Online]. https://doi.org/10.6028/NIST.SP.800-126r3 , 2018.

[71] Riigi Infosüsteemi Amet (RIA), *Estonia ID1 Chip/App: Technical Description*, https://www.id.ee/wp-content/uploads/2020/10/td-id1-chip-app-1.pdf, 2018.

[72] CEN, *CEN/TS 15480-2:2012 Identification card systems - European Citizen Card - Part 2: Logical data structures and security services*, https://www. evs.ee/en/cen-ts-15480-2-2012, 2012.

[73] A. Parsovs und D. Morgan, „Using the Estonian Electronic Identity Card for Authentication to a Machine , Nov. 2017, pp. 175–191. doi: 10.1007/978-3-319-70290-2_11.," in *Secure IT Systems. NordSec 2017. Lecture Notes in Computer Science*, 2017.

[74] NIST, „FIPS 140-2, Security Requirements for Cryptographic Modules," [Online]. https://csrc.nist.gov/publications/detail/fips/140/2/final, 2001.

[75] NIST, “SP 800-115: Technical Guide to Information Security Testing and Assessment,” [Online]. https://nvlpubs.nist.gov/nistpubs/Legacy/ SP/nistspecialpublication800-115.pdf, 2008.

[76] Infineon Technologies AG, “Security IC Platform Protection Profile with Augmentation Packages,” [Online]. https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf, 2014.

[77] CEN, “CEN prEN 14169-1:2010 Protection profiles for secure signature creation device — Part 1: Overview,” [Online]. https://infostore.saiglobal.com/preview/98702491388.pdf?sku=878513_SAIG_NSAI_NSAI_2087711, 2012.

[78] ISO/IEC, “ISO/IEC 30107-3:2017, Information technology — Biometric presentation attack detection — Part 3: Testing and reporting,” [Online]. https://www. iso.org/obp/ui/#iso:std:iso-iec:30107:-3:ed-1:v1:en, 2017.

[79] ISO/IEC, „ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements,“ [Online] url: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en, 2013.

[80] The PTES Team, „The Penetration Testing Execution Standard Documentation Release 1.1,“ [Online]. https://buildmedia.readthedocs.org/media/pdf/pentest-standard/latest/pentest-standard.pdf, 2017.

[81] A. Countant, “French Scheme CSPN to CC Evaluation”.

[82] R. A. Caralli, J. A. Stevens, L. R. Young and W. R. Wilson, “Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process,” CERT, 2007.

[83] C. J. Alberts, A. J. Dorofee, J. F. Stevens and C. Woody, “OCTAVE-S Implementation Guide, Version 1,” 2005.

[84] CERT SEI, “Android Secure Coding Standard,” [Online]. https://wiki.sei.cmu.edu/confluence/display/android/Android+Secure+Coding+Standard.

[85] NCCGroup, “CERT C Programming Language Secure Coding Standard,” 2007.

[86] F. Long, D. Mohindra and R. C. Seacord, “The Cert Oracle Secure Coding Standard for Java, 1st edition,” ADDISON WESLEY PUB CO INC, Upper Saddle River, NJ, 2011.

[87] A. Ballman, “SEI CERT C++ Coding Standard Edition, The: 98 Rules for Developing Safe, Reliable, and Secure Systems: 98 Rules for Developing Safe, Reliable, and Secure Systems in C++,” 2016.

[88] Weibull, “Basic Concepts of FMEA and FMECA,” [Online]. http://www.weibull.com/hotwire/issue46/relbasics46.htm.

[89] ISO/IEC, “ISO/IEC 19790:2012 Information technology — Security techniques — Security requirements for cryptographic modules v2,” [Online]. https://www.iso.org/obp/ui/#iso:std:iso-iec:19790:ed-2:v2:en, 2015.

[90] „Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components,“ [Online]. https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf, 2017.

[91] ENISA, “Considerations on ICT security certification in EU: Survey Report,” https://www.enisa.europa.eu/publications/certification_survey, 2017.

[92] NIST, “SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,” [Online]. https:// nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800- 137.pdf, 2011.

[93] NIST, „NISTIR 8011, Automation Support for Security Control Assessments, Volume 1: Overview,“ [Online]. https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8011-1.pdf, 2017.

Annex A: Certification Involvement of the Project Partners and Associated Entities

To get feedback about the methods used in practice and the challenges involved, we asked the project partners and associated entities in Europe to answer the questionnaire included in Annex B of this deliverable. We received 38 replies to the questionnaire from 31 different institutions. Of the 38 replies, 28 answers were sent by individuals who are affiliated with the CyberSec4Europe project. We estimate that this is mainly due to the fact that certification is not too prevalent among the project partners. From the associated entities that we managed to reach, only expert level people answered the questionnaire.

Of the answers, 20 were from academic institutions, 12 were industry partners (2 SMEs, 2 micro-SMEs and 7 large industry partners) and 6 answer from another category (a non-profit organisation, a government institution, 2 financial institutions, and 2 research and training institutions).

Most of the answer options were non-exclusive, so the responder could choose all the options that they thought were right.

A.1 Academia

A.1.1 Certified Assets

Most of the responders (14) are not aware of any part of the organisation holding certificates for information security management system (ISMS) (e.g. ISO/IEC 27001), employees (e.g. CISA), software (e.g. CC), hardware (e.g. CC), offices, infrastructure or services (e.g. the organisation's data centre or cloud service is ISO/IEC 27k certified). Four responders indicated that their employees have certificates (e.g. ISACA CISA and CISM, CISO). One has hardware certified under Common Criteria (CC), and two have ISO/IEC certifications on their offices, infrastructure or services.

A.1.2 Certification Services

Again, most of the responders (11) are not aware of their organisation providing certification services. One organisation provides authorisation services for the Finnish nationally recognised cyber security certification scheme called FINCSC – Finnish Cyber Security Certificate[30]. One organisation researches certification tools and methodologies and another provides MSc courses in collaboration with third parties teaching ISO/IEC 27001 certification methods to MSc students in cyber security.

A.1.3 Reliance upon Certification Schemes

Three organisations reported their reliance on Common Criteria as a certification scheme. One also referenced NIST FIPS140-2 (Security Requirements for Cryptographic Modules) and another referenced the following certification standards that they rely upon: ISO/IEC 31000 (Risk Management), ISO/IEC 29119 (Software and systems engineering — Software testing), ETSI EG 203 251 (Methods for Testing & Specification; Risk-based Security Assessment and Testing Methodologies). The other responders either were not sure or said that they did not rely on any schemes.

A.1.4 Testing Approaches

We asked what kinds of testing approaches the organisation uses and of those who answered that their team uses testing approaches, all mentioned penetration testing, model-based testing, and fuzzing. Six also mentioned static code analysis. One also relies upon formal verification to ensure the correctness of their development. Moreover, one responder specifically researches testing and verification.

[30] https://www.fincsc.fi/en/services/

A.1.5 Tools for Achieving Compliance

We asked which of the given tools the organisation uses for achieving compliance. Most (14) responders were not sure or did not think their organisation used any tools.

The tools mentioned by the other responders were open-source penetration testing tools, CertifyIt, Rational Software Architecture, TITAN, JUnit, Wireshark, FIT IoT Lab, LINDDUN, SPARTA, and NIST STS randomness statistical testing suite. One responder said that their organisation has their own custom tools for achieving compliance in addition to the ones we proposed as examples. Also OneDrive, version control (git, svn), and additional components of MS Teams were brought out as examples.

A.1.6 Risk Assessment Schemes

Finally, we asked about the risk assessment schemes that the organisations use. Most of the partners were not sure about this process in their organisation but six responders mentioned that they use CVSS (Common Vulnerability Scoring System), two mentioned CWSS (The Common Weakness Scoring System), and one mentioned FAIR (Factor Analysis of Information Risk). One responder said that they use their National Framework for their risk assessment process.

A.2 Industry

A.2.1 Certified Assets

Of the 12 industry partners, seven hold a certificate for the information security management system (ISMS) (namely, ISO/IEC 27001). Six responders said that their organisations have CISA certified employees. Industry partners also hold certificates under CC for customer software and the large companies hold certificates in most or all of the domains that we specified, namely ISMS (ISO/IEC 27001), employees (e.g. CISA, CISSP), software and hardware (CC), and offices, infrastructure or services.

A.2.2 Certification Services

Four responders said their organisations provide GDPR related audits, and in addition, three of these provide third-party audits. Privacy impact analysis and internal certifications/training programs were mentioned. Three organisations (all large companies) issue certificates as well.

A.2.3 Reliance upon Certification Schemes

Industry partners mostly (7) rely on Common Criteria as a certification scheme. In addition, the European NIST FIPS140-2, Privacy Seal (EuroPriSe), UL CAP (UL Cybersecurity Assurance Program), and CSPN (Certification de Sécurité de Premier Niveau) were indicated.

A.2.4 Testing Approaches

The most used testing method indicated by the industry responders was penetration testing (8), but also static code analysis (6), fuzzing (4), and model-based testing (3) were mentioned.

A.2.5 Tools for Achieving Compliance

From the industry responders, seven use tools for managing ISMS compliance information (e.g. version control, task management, wiki, spreadsheets), tools testing security (including cryptographic) systems and tools for supporting the audit process. Several responders indicated that their organisation uses proprietary tools for achieving compliance, however, most responders did not know in detail, which tools were in use.

A.2.6 Risk Assessment Schemes

For risk assessment, five responders were not sure about this process in their organisation but six responders mentioned that they use CVSS (Common Vulnerability Scoring System), four mentioned CWSS (The Common Weakness Scoring System), and two mentioned FAIR (Factor Analysis of Information Risk). One responder also mentioned DO-326A.

A.3 Other

The non-profit organisation indicated that they are planning to certify digital solutions that are complying with the OASC Minimal Interoperability Mechanisms. They will not carry out the certification itself; this will be done by a third-party. The rest of the subsection looks at the other five responders.

A.3.1 Certified Assets

All of the responders (5) indicated that their organisations hold certificates for information security management system (ISMS) (e.g. ISO/IEC 27001). Three also indicated certificates for employees, two software (e.g. CC), and two for hardware (e.g. CC). The specified certificate list in this category was long: ISO 9000, 14001, 17025, 20000, 20400, 22222, 27001, 37001, 30000, 37301, 45001, CC, CISP, CISA, CISM, CRIS, CPMP, CEH.

A.3.2 Certification Services

Only one organisation indicated that they provide third-party audits for trust services (ISO 17025). They also issue certificates for this process. Others were not aware that their organisation provided any certification services.

A.3.3 Reliance upon Certification Schemes

Two of the responders were not sure which certification schemes their organisation relies upon, however two indicated CC, one indicated ISO/IEC 27001, and one indicated LINCE.

A.3.4 Testing Approaches

Five responders mentioned penetration testing, three mentioned static code analysis, two mentioned fuzzing and one model-based testing and dynamic analysis.

A.3.5 Tools for Achieving Compliance

Four responders indicated that they use tools for managing ISMS compliance (dedicated data management software, version control, task management, wiki, spreadsheets), three used tools for testing security (including cryptographic) systems, and one used tools for supporting the audit process.

A.3.6 Risk Assessment Schemes

Three responders mentioned that they use CVSS and two mentioned CWSS. One also mentioned Octave and FAIR. In addition, Severity, Exposure, Probability (SEP) and MAGERIT were brought out.

Annex B: Certification Involvement Questionnaire

CyberSec4Europe Partner Certification Involvement Questionnaire

Fields marked with * are mandatory.

Dear CyberSec4Europe partner!

This questionnaire for Task 7.3 (Deliverable 7.7) studies cybersecurity and IT security certification activities in the partner organisations of CyberSec4Europe. The questionnaire should not take more than 5-15 minutes of your time (15 if you have to look up tool names).

Thank you for taking the time to help us!

Partner description

* Organisation name

* Organisation type
- Academia
- Industry
- Other

Size of organisation
- Micro-SME
- SME
- Large company

Please specify organisation type

What is your level of confidence for the topic of certification in your organisation?
- Expert
- Pretty good
- Some knowledge
- Not confident at all

1

Cybersecurity and IT security Certification Activities

* Does your organisation hold certificates for the following?
  - ☐ Information Security Management System (ISMS) (e.g. ISO/IEC 27001)
  - ☐ Employees (e.g. CISA)
  - ☐ Software (e.g. CC)
  - ☐ Hardware (e.g. CC)
  - ☐ Offices, infrastructure or services (e.g. your organisation's data center or cloud service is ISO/IEC 27k certified)
  - ☐ None that I am aware of

* Please specify which certificates

* Does your organisation provide certification services?
  - ☐ None that I am aware of
  - ☐ Third-party audits
  - ☐ GDPR related audits
  - ☐ Using automated certification tools
  - ☐ Other

* Please specify which services

* Does your organisation issue security certification of products or processes? Do you issue certificates to experts?
  - ○ Yes
  - ○ No

* Specify the certificate you are awarding.

Certification Approaches and Tools

* Which certification schemes does your organisation rely upon?
  - ☐ CC (Common Criteria)
  - ☐ CSPN (Certification de Sécurité de Premier Niveau)
  - ☐ UL CAP (UL Cybersecurity Assurance Program)
  - ☐ Commercial Product Assurance (CPA)
  - ☐ European Privacy Seal (EuroPriSe)
  - ☐ NIST FIPS140-2
  - ☐ Other

2

- [ ] Not sure
- [ ] N/A

* Please specify which schemes

* What kind of testing approaches does your organisation use?

- [ ] Penetration testing
- [ ] Model based testing
- [ ] Fuzzing
- [ ] Static code analysis
- [ ] Other
- [ ] Not sure
- [ ] N/A

* Please specify which approaches

* What kind of tools does your organisation use in the process of achieving compliance?

- [ ] Tools for managing ISMS compliance information (e.g. version control, task management, wiki, spreadsheets)
- [ ] Tools testing security (including cryptographic) systems (e.g. NIST STS randomness statistical testing suite, Riscure Inspector Side Channel Analysis, ChipWhisperer)
- [ ] Tools for supporting the audit process
- [ ] Tools for training and knowledge transfer for best practices (e.g. GDPR training tools)
- [ ] Other
- [ ] Not sure
- [ ] N/A

* Please specify which tools

* What kind of risk assessment schemes does your organisation use?

- [ ] CVSS (Common Vulnerability Scoring System)
- [ ] CWSS (The Common Weakness Scoring System)
- [ ] Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
- [ ] FAIR (Factor Analysis of Information Risk)
- [ ] Other
- [ ] Not sure
- [ ] N/A

* Please specify which schemes