UNIVERSITY OF TARTU
Institute of Computer Science
Cybersecurity Curriculum

Jayavarshini Thirumalai

An integrated approach for certification and re-certification based on the case study of an integrated circuit

Master's Thesis (24 ECTS)

Supervisor: Liina Kamm, PhD (Cybernetica AS)
Supervisor: Mari Seeba, MSc

Tartu 2021

An integrated approach for certification and re-certification based on the case study of an integrated circuit

Abstract: A system is expected to undergo necessary security assessment to ensure that it is in compliance with the baseline security requirements. Otherwise it becomes hard to trust that the product is secure enough to use. For this purpose, certification can be used to ensure that a system is secure and safe to use. In this thesis, we define an integrated approach that aims to reduce time and cost in the product evaluation process by refining and integrating existing approaches. Hence, we consolidate solutions from the ARMOUR methodology, the ECSO meta-scheme and the NIST SP 800-137 to support certification and re-certification. We use a case study of the integrated circuit (or chip) as an example. In addition, we follow the Common Criteria based European Cybersecurity Candidate Scheme guidelines from ENISA to define a standardized process in certifying and re-certifying the product. Three different validators validated the thesis through face validity.

Keywords: cybersecurity certification, ECSO, ETSI, NIST, ENISA, certification schemes, Common Criteria, ISO/IEC 19790, model-based testing, penetration testing, risk assessment, monitoring, re-certification, incremental certification, cybersecurity labeling, automation.

CERCS: T120 Systems engineering, computer technology

Sertifitseerimise ja taassertifitseerimise integreeritud lähenemine kiibi juhtumianalüüsi näitel

Lühikokkuvõte: Selleks, et tagada susteemi vastavus turbe põhinõuetele, peab hindama süsteemi turvalisust. Vastasel juhul on raske süsteemi toimivust usaldada. Susteemi usaldusväärsuse tõendamiseks kasutatakse sertifitseerimist. Selles magistritöös kirjeldame integreeritud lähenemisviisi, mis kasutab ja täiustab olemasolevaid lahendusi ning mille eesmärk on vähendada süsteemi hindamisele kuluvat aega ja raha. Oma sertifitseerimise ja taassertifitseerimise protsessi loomiseks kasutame põhimõtteid ARMOURi metoodikast, ECSO metaskeemist ja juhendist NIST SP 800-137. Juhtumianalüüsiks kasutame kiipi. Lisaks järgime toote sertifitseerimisel ja taassertifitseerimisel ENISA Euroopa Küberturbe Kandidaatskeemi (EUCC) juhiseid, mis põhinevad Ühiskriteeriumitel (CC). Kolm erinevat spetsialisti valideerisid lõputööd intervjuude käigus.

Märksõnad: küberturbe sertifitseerimine, ECSO, ETSI, NIST, ENISA, sertifitseerimisskeemid, Ühiskriteeriumid (CC), ISO/IEC 19790, mudeltestimine, läbistustestimine, riski kaalutlemine, seire, taassertifitseerimine, sammsertifitseerimine, küberturbe märgis, automatiseerimine.

CERCS: T120 Süsteemitehnoloogia, arvutitehnoloogia

Contents

Acknowledgements

I would like to first acknowledge the guidance and constant support from my supervisors Dr. Liina Kamm from Cybernetica AS and Mari Seeba from University of Tartu throughout the research work. Your encouragement and feedback helped me in formulating the thesis to a great extent.
I also would like to acknowledge the validators, Dr. Sara Nieves Matheu Garcia from University of Murcia, and Dr. Jan Villemson and Dr. Aivo Kalu from Cybernetica AS for your time and discussions during the thesis validation. Your expertise and suggestions helped me in expressing my thesis more clearly and concisely.
I wish to extend my special thanks to Cybernetica AS, TalTech University and University of Tartu for the opportunity to learn and gain knowledge in various aspects of cybersecurity. This work has been supported by the EU H2020-SU-ICT-03-2018 Project No. 830929 CyberSec4Europe (cybersec4europe.eu).

List of Figures

List of Tables

Abbreviations

- **CAS** Certificate authorizing scheme
- **CC** Common Criteria
- **COTI** Challenges of the Industry
- **CSA** Cybersecurity Act
- **CVE** Common Vulnerabilities and Exposure
- **CVSS** Common Vulnerability Scoring System
- **CWSS** Common Weakness Scoring System
- **ECSO** European Cyber Security Organization
- **ENISA** European Union Agency for Cybersecurity
- **ETR** Evaluation technical report
- **ETSI** The European Telecommunications Standards Institute
- **EUCC** European Candidate Cybersecurity Certification Scheme
- **FIPS** Federal Information Processing System
- **IAS-ECC** Identification Authentication Signature-European Citizen Card
- **ITSEF** IT Security Evaluation Facilities
- **MBT** Model-based testing
- **NIST** National Institute of Standards and Technology
- **NISTIR** National Institute of Standards and Technology Interagency or Internal Reports
- **NVD** National Vulnerability Database
- **PII** Personally identifiable information
- **PKI** Public key infrastructure
- **PPA** Politsei-ja Piirivalveamet
- **QSCD** Qualified Signature Creation Device

- **RIA** Riigi Infosüsteemi Amet
- **SOTA** State Of The Art Syllabus
- **SUT** System under test
- **TOE** Target of evaluation

1 Introduction

The physical world is evolving into the digital era where a lot of activities are processed digitally such as digital signing, digital identities, digital processing of personally identifiable information (PII). In addition to the benefits like automation and remote connectivity, digital activities lead to various issues concerning privacy and security of the data. Now it has become difficult to trust some of the digital systems like services, products, information systems or solutions containing all of these. Conformity of these digital systems can be assured through certification. Based on the NIST definition, the term certification in this thesis is referred as, the security assessment of a system in terms of administration, operational and technical to ensure that controls are implemented properly and are in compliance with the baseline security [41]. In general, a certificate of a product ensures that the product has undergone various performance or quality assurance tests to verify its conformity to the set of specifications or criteria defined in the certification scheme. The various schemes and standards such as Common Criteria [11], ISO/IEC 27001 [27] are available for assessing the security strength of an item to ensure conformity. Each scheme provides different functionalities and has different advantages, but there is no single scheme that fits every requirement.

1.1 Purpose and Scope

The purpose of this thesis is to research the possibility of a refined, semi-automated and cost-effective certification and re-certification process. To support the process, a case study on the Estonian ID card chip is used in terms of functionalities, vulnerabilities and certification schemes and standards.
The certification and re-certification processes will be limited to the integrated circuit. The attackers make use of sophisticated and automated attack methods to compromise the targets. Hence the thesis discusses the possibility of semi-automating the security control assessments on the chip to identify and mitigate threats sooner. A single certification scheme cannot fulfill all the security requirements of a product, hence this research work makes use of the integrated solution proposed by the ECSO meta-scheme [16]. This allows different certification schemes or security standards to be combined to carry out the certification or re-certification assessments of the chip reliably. The process flow for certifying and re-certifying the chip is based on the ARMOUR methodology [6]. The scope of the research work presented in this thesis is currently limited to the theoretical level.

1.2 Research Problem

The integrated circuit or chip is one of the primary components used in almost every computing device, as it is a sector independent ICT product. All the chips and the processes involved are CC certified. Yet the chip has been found vulnerable to various attacks which can have a wide impact on different sectors. An example is mentioned in Section 2.1.2. We will look at the possibilities of integrating three different frameworks: the meta-scheme [16] approach from ECSO, the ARMOUR methodology [6] developed based on one of the ETSI proposals [21] and the NIST SP 800-137 [38] in such a way that a standardized approach can be described to support the chip certification and re-certification.

Research questions:
RQ1: How to define the certification and re-certification of the chip using national or international schemes or standards at minimal time and cost?

RQ1.1: How to describe the testing process?

RQ1.2: How to semi-automate the security control assessment?

RQ1.3: How to reduce the time and cost taken during re-certification?

RQ1.4: How to improve the transparency of a properly certified chip?

RQ1.5: How to modify the approach defined in this thesis to support all kinds of products?

1.3 Novelty

The novelty of this research work is the integration of solutions taken from different organizations like ETSI, ECSO and NIST for ensuring the conformity of the chip along with the consideration of the ENISA guidelines [20] on cybersecurity certification throughout the research work.

1.4 Document Structure

The author has constructed the thesis in the following format, Section 2 describes the background information. Section 3 defines our integrated approach for the ID card chip. Section 4 deals with the validation results of the research. Finally, Section 5 talks about the conclusions and future work.

2 Background Information

2.1 Estonian ID Card

To illustrate the idea of our integrated approach, we are using the Estonian ID card chip as a basis for our examples. The Estonian ID card is a mandatory document for all Estonian citizens and people who are planning to stay in Estonia. It is a primary identification document and accepted throughout the European Union (EU) countries. This document can be used in different forms for example as an identity document, for digital signatures, as a residence permit card and as a travel document. The ID cards are issued by the Police and Border Guard Board (Politsei-ja Piirivalveamet, PPA) based on the Identity Documents Act (IDA).

Initially PPA contracted with Gemalto[1] (formerly Trüb Baltic AS) for manufacturing the ID cards. But the after the Estonian ID card crisis (Section 2.1.2), PPA contracted with IDEMIA[2], a French company. The card manufacturer subcontracted with the qualified TSP (Trust Service Provider) called SK ID Solutions AS[3] for issuing the digital certificates to the ID card. This TSP is working under the legislation of eIDAS. The Estonian Information System Authority (Riigi Infosüsteemi Amet, RIA) is responsible for collecting requirements or applications required for using the eID services. The technical features of the chip are described in the following section.

2.1.1 Technical Details

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 (PKI) 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 (QSCD) certified based on various Protection Profiles that are listed in Section 2.7.1. This IAS-ECC meets all the requirements of the CEN/TS 15480-2 [9] (European eID) documents. Thus, it can implement the security and functional use cases through various authentication mechanisms [1]. 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 [44].

[1] https://en.wikipedia.org/wiki/Gemalto
[2] https://www.idemia.com/
[3] https://www.skidsolutions.eu/en

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 chips. The attackers usually make use of physical parameters such as electromagnetic emission, execution time, power consumption to perform side-channel attacks.

Vulnerable RSA generation (CVE-2017-15361). Initially, the Estonian ID cards used chips produced by Infineon Technologies AG[4]. These chips were using a vulnerable software library which led to the practical factorization 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 [34]. 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 may 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.

We listed a set of threats or vulnerabilities (Section 3.2) based on the described attacks and features of the chip. We also considered certain vulnerabilities related to the chip functionalities from the NIST Vulnerability Database[5]. There are various attacks which are not in the scope of the thesis but can be considered for future work.

2.2 ARMOUR Methodology

The ARMOUR methodology [6] is developed using one of the ETSI proposals [21]. It integrates ISO 31000 [25], extended control assessment and the testing actions defined in ISO/IEC/IEEE 29119-1 [29]. The two major underlying themes are security testing and security risk assessment where the results of one process can be used to improve the other. Both are initiated by a process called establishing the context. The results of these activities can be managed for any changes or updates and shared by the processes called monitoring and review and communicate and consult.

Our integrated approach is developed by adopting certain steps or processes from the ARMOUR methodology. From Figure 1, we used the concept of

[4]https://www.infineon.com/

[5]https://nvd.nist.gov/

establishing the context, security assessment and communicate and consult. In defining the planning phase of our integrated approach (Section 3.3), we used the terms and processes from Figure 1. In addition, our integrated approach represents the communicate and consult process as communicating the results (Section 3.6). All the processes involved in the ARMOUR methodology are represented on Figure 1.

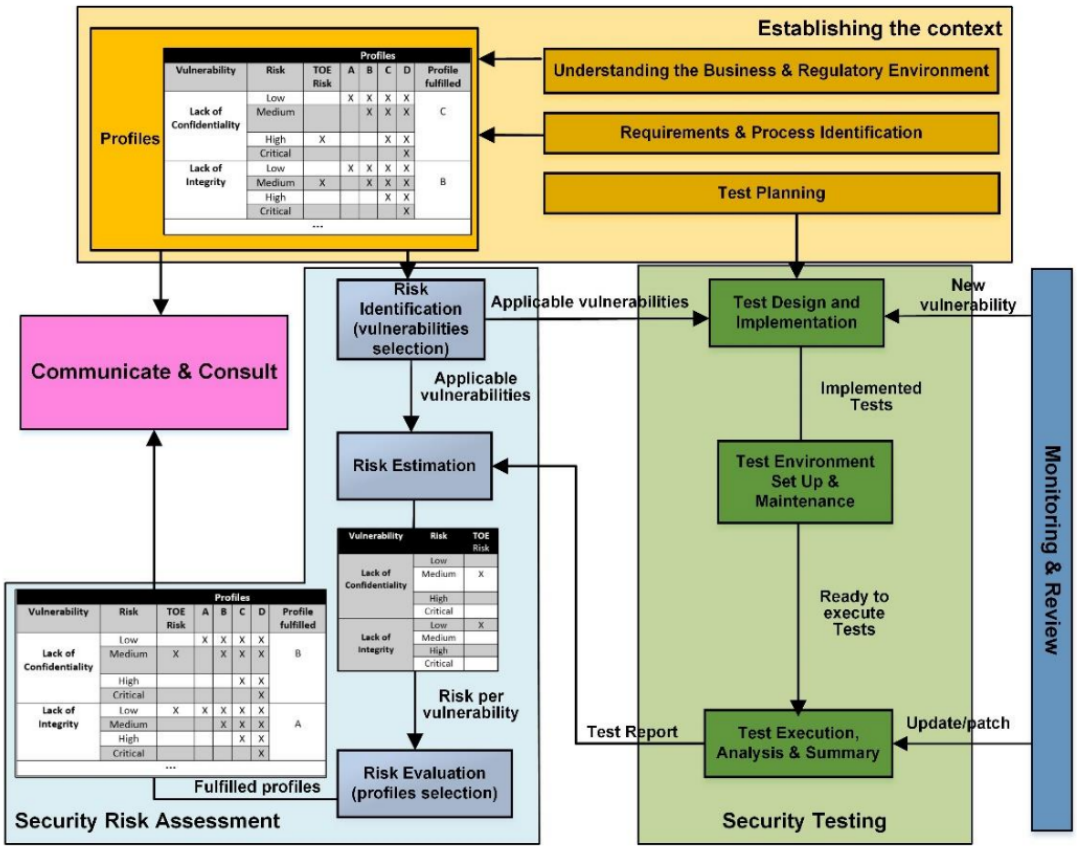

Figure 1. ARMOUR methodology [6].

2.3 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 [20] from ENISA provides a set of guidelines, rules and regulations based on Common Criteria for an ICT product evaluation. These guidelines are in compliance with the requirements of the Cybersecurity Act [2]. By following these guidelines, we can

define a standardized framework that support multiple ICT products. The major benefits of implementing standardized criteria and methods for cybersecurity evaluation are, for example, consistency between different manufacturers and vendors, re-usability, harmonization of terminology, awareness [2]. ENISA surveyed on the considerations for ICT security certifications. Based on the survey report [19], we developed Table 1 which represents the issues that can be solved through our integrated approach.

Table 1. Certification issues and their solutions.

ENISA considerations	**Solution used in the research**
Lack of transparency	cybersecurity label
Lack of certification support for the life-cycle of the product	Incremental certification
Cost and time	Incremental certification

In our integrated approach, we are using the EUCC guidelines throughout the process starting from the selection of assets to the re-certification process. Hence, our integrated approach is in accordance with CSA Articles.

2.4 ECSO Meta-scheme Approach

European Cyber Security Organization[6] (ECSO) is a non-profit organization which was established in 2016. The major goal of ECSO is to provide standardized cybersecurity solutions for supporting and protecting the digital processes. One of the results from ECSO Workgroup 1 (WG1) is the meta-scheme approach (Standardisation, certification and supply chain management). The meta-scheme approach focuses on two concepts: security and privacy. In this approach, two WG1 documents, Challenges of the Industry (COTI) [15] and State of the Art Syllabus (SOTA) [18] are compared to address drawbacks in existing schemes and standards.

The ECSO meta-scheme [16] involves the integration of various certification schemes or standards for the conformity of items. It can be achieved by defining a high-level common language or format across the schemes selected for evaluation. The expert group (EG) is responsible for defining the common language where the EG represents security researchers or specialists. For evaluating an item, it is significant to understand the scope of the target from which the EG will be drawing related threats, make assumptions, choose relevant standards and more. Thus, some modified notions are cascaded from Common Criteria. Initially, a

[6]https://ecs-org.eu/

Generalized Protection Profile (GPP) is defined in the common language for the security target. A GPP is composed of the following terms [16]:

- The security problem definition that deals with defining the assets, their threats, assumptions, constraints,
- Security objectives that deal with identifying the security requirements,
- Security services and features related to the functionalities of the target,
- Instantiation of the levels talks about the selection of schemes from SOTA,
- Visual representation of the minimum required scope of security functionality per level using the cybersecurity label,
- Additional evaluation includes the steps that have to be defined.

The developed GPP has to be approved by the accredited third party. Similar to GPP, the meta-scheme uses the terminology Generalized Security Target (GST) to represent the target to be evaluated. Assurance level is generated based on the type of penetration testing carried out (black-box, white-box and gray-box) on the target. The relation between the scope of the security functionality and the assurance level helps the EG to appropriately select and modify the schemes available from SOTA [18] for the identified issues. A drawback with the meta-scheme approach is that there is no common platform or database to share the findings and results. This is not considered a trivial issue to manage. Also, there are no discussions about the re-certification or monitoring processes. But unlike ARMOUR methodology, this approach is more general and allows the certification of different products and services (not only IoT devices). Thus, solutions from two different approaches can complement each other when integrated.

From the meta-scheme, we use a common language (GPP) to select and integrate the appropriate certification schemes or standards for chip evaluation. The term EG is also adopted by us to represent the security researchers of this research work. Further discussions can be found in Section 3.

2.5 ECSO State of the Art Syllabus

The ECSO SOTA [18] is a publicly available dynamic document which consists of all the available certification schemes used for security certification and also standards that are related to cybersecurity for various assessments. The SOTA document helps in providing certification to a component or a part of the component, products and organization. For every scheme or standard and specification, the SOTA document provides brief descriptions for the following

terms focus, applicable area, associated scheme and governance (talks about the existing scheme that evaluates products or processes against the corresponding standard), process, practice and relation to other standards or schemes [16].

2.5.1 Selected Evaluation Schemes

The certification schemes or standards provide a set of regulations or guidelines. Based on these the conformity of a product or any system is approved or denied. The certification schemes are required to be generic rather than sector dependent, since the technologies that are used in developing a solution may be used in multiple domains. We used the following schemes in our integrated approach for evaluating the ID card chip. These schemes are taken from the SOTA [18].

Common Criteria. Common Criteria for Information Technology Security Evaluation (CC) is one of the international standards under ISO/IEC 15048 [11]. Initially, a Protection Profile (PP, Section 2.7.1) is created based on the domain and scenario of the security target. It defines a set of security functional requirements [12], security assurance requirements [13] and guidelines for conducting security evaluation on security targets (a refinement of PP). Through Evaluation Assurance Level (EAL), CC shows the level of assurance, strictness and severity carried out during the target evaluation. The target of evaluation (TOE) is validated by IT Security Evaluation Facilities (ITSEF). The resulting document, the evaluation technical report (ETR) is sent to the certificate authorizing scheme which decides whether to issue the CC certificate to the product. This certificate authorizing scheme has recognized testing laboratories for carrying out an assessment on the target and validates ETR.

ISO/IEC 19790 Cryptographic module standards. This is an international standard developed based on the FIPS 140-2 [36]. It is used for defining the security requirements for cryptographic modules through four security levels. The standard specifies 11 areas [18] 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 [26].

The idea of our integrated approach is to combine the requirements of CC (as base scheme) and ISO/IEC 19790 using the Generalized Protection Profile (GPP). We integrated 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 recognized worldwide. ISO/IEC 19790 is integrated with CC because the ID card chip is constituted of cryptographic features. Our integrated approach provides a

higher level of assurance than using a single evaluation scheme or standard.

2.6 Security Control Assessments

NIST SP 800-53A [40] defines three different assessment methods: examine, interview and test. The examine assessment method is more time consuming. The interview method requires manual work to achieve good results. The test method is the most effective for automation and provides more accurate results with proper implementations [43]. In our research, we are using the test assessment method as it the most feasible option.
As the assessment method is chosen, we need to decide on the assessment types. The following sections explain the different types of assessments and the features based on EUCC [20] and the ECSO meta-scheme [16].

2.6.1 ECSO Assessment Options

Some organizations carry out self-attestation which is either a declaration without any assessments or declarations based on a self-assessment or third-party assessment. A product or a system can be assessed in three different ways [17].
Self-assessment. Generally, self-assessment is not considered as an effective assessment approach. As defined in the Cybersecurity Act (CSA) article 54.1 [2], we need to verify whether self-assessment is accepted by the schemes. For instance, self-assessment is allowed only in the basic assurance level and this level is not accepted by the EUCC scheme [20]. It is hard to predict whether the self-assessment was accredited, as it is carried out by the organization itself.
Third-party assessment. Unlike self-assessment, third-party assessment is carried out by an accredited third-party. It can be carried out by either an in-house body or external body. The in-house assessment is led by the organization and the involved activities are validated by the National Accreditation Body or an accredited third-party. External assessment is carried out by an accredited third-party and the activities are inspected by the national accreditation body .
National third-party assessment. This type of assessment is generally carried out by the national entity for ensuring national security for example in the case of military and nuclear projects.
In our approach, self-assessment is not accepted as a legitimate evaluation. Hence we have defined the security assessments in a way that are carried out by an conformity assessment body (CAB) or accredited third-party [20]. This testing laboratory is referred as IT Security Evaluation Facilities (ITSEF) or tester in the thesis. As a result of an assessment, it is possible to evaluate whether the security objectives, assurance level and selection of security schemes

are in accordance with the CSA Articles 51, 52 and 54 respectively [2].

2.6.2 Testing Approaches

The fundamental goal of security testing is to ensure that the software meets the requirements for major security properties such as confidentiality, integrity, availability, authentication, authorization and non-repudiation. The system under test (SUT) can be a system, service, application or any other digital item which is being tested with the baseline security controls. To select the appropriate testing techniques, we have analyzed the features, pros and cons of various testing methods from [32]. The following two approaches have a significant role in our integrated approach.

Model-Based Testing. The Model-based testing (MBT) [32] helps us to design and create an efficient model that represents the SUT, its environment and its behaviour. One of the main advantages of MBT is that we can partially automate the re-certification process. MBT is carried out by designing the models using a high-level representative language such as Object Constraint Language (OCL) [7] or UML. Designing of this test model is carried out manually. Based on the designed model, the test steps are portrayed using the same. But test cases can be generated automatically [46]. There are various tools such as CertifyIt and MISTA for generating the tests [31].

Penetration Testing. Penetration testing [5] can be used to simulate real-time attacks for detecting vulnerabilities and exploit them. The testing can be black-box, white-box or gray-box and requires high technical knowledge and skill for carrying out them. In black-box penetration testing, we have to start from the information gathering process on the target and simulate an outsider attack. In white-box penetration testing, we are provided with sufficient information about the target like network architecture, source code for carrying out the test. In gray-box penetration testing, we have partial knowledge about the target like admin account credentials and simulate a combination of internal and external testing. In addition, other testing approaches [32] may be carried out as part of penetration testing based on the SUT requirements. For instance, experts may carry out source code analysis [14] or fuzzing [10] during a web application penetration testing to improve code quality. Some examples of documentation or manual for carrying out penetration testing like Open Source Security Testing Methodology Manual (OSSTMM) [24], Penetration Testing Methodologies and Standards (PTES) [47], Open Web Application Security Project (OWASP)[7] testing guide.

The testing methods can be combined, for instance, MBT can be combined with fuzzing [45] to provide an efficient method. We are using a combination of

[7]https://owasp.org/www-project-web-security-testing-guide/v42/

MBT and penetration testing in our integrated approach. ITSEF is responsible for this testing. Also, ITSEF should follow the PTES documentation [47] while carrying out penetration testing. We selected PTES as it is more generic than other documentations (like OSSTMM, OWASP) but specific to penetration testing. The testing process is described in Section 3.4.

2.6.3 Risk Assessment

The risk assessment process helps an organization to create better business continuity and disaster recovery plans by analyzing the threats associated with valuable assets. Risk assessment can be of three types: quantitative, semi-quantitative and qualitative [39]. The organization can choose the appropriate assessment type based on their business process or environment. There are various risk assessment approaches such as the Common Weakness Scoring System (CWSS) [33], the Veracode Rating System[8], the OWASP risk rating methodology[9] and the Common Vulnerability Scoring System (CVSS) [23].

The CVSS [23] is an open-source framework which provides three groups of metrics: base, temporal and environmental. Initially, we can calculate the base metric based on exploitability metric and impact metric. This base metric is represented as a numerical value in the range of 0.0 and 10.0, but this can be changed based on the temporal and environmental metric scores. CVSS allows the representation of these scores through text (like low, medium and high). CVSS v3.1 is the latest version in which the functionality of metrics is modified to some extent. The CVSS is used in various platforms including Common Vulnerabilities and Exposures (CVE) created by the MITRE corporation[10] and the NIST Vulnerability Database created by NIST.

Our integrated approach uses a semi-quantitative risk assessment. To support risk communication, the generated risk scores (quantitative) can be mapped to the severity levels (qualitative). We are using CVSS v3.1 to generate the severity levels of the exploitable vulnerabilities.

2.7 Additional Elements

2.7.1 Protection Profiles

As discussed in Section 2.5.1, PPs are developed to represent the different contexts or scenarios of the security target. EUCC [20] and CC [18] prefers the PPs to be certified first before using them to certify a product. In addition,

[8]https://help.veracode.com/r/DGHxSJy3Gn3gtuSIN2jkRQ/civ7DGQfn2Kk4xh4Cz4UtA

[9]https://owasp.org/www-community/OWASP$_{R}isk_{R}ating_{M}ethodology$

[10]https://www.mitre.org/

EUCC requires each certified PP certificate to contain information like a unique certificate ID for the PP and technical and non-technical details of the PP. For instance, existing PKI application of Estonia eID documents are certified for the following PPs [1]:

- 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.

In this thesis, the term GPP is used for representing integrated PPs. The EG can either make use of the existing PPs or a GPP is developed based on the Common Criteria PPs, requirements of ISO/IEC 19790 [26] or other related PPs. The developed GPP is then certified by the accredited testing laboratory (ITSEF) to verify whether they are in compliance with the CC requirements. This is further discussed in Section 3.3.

2.7.2 Cybersecurity Label

Lack of transparency is one of the issues mentioned by ENISA to consider during the security certification of any ICT product [19]. When the chip is certified successfully, we can create a label which is valid until a specific period of time. Labelling increases the transparency about the security assurance of the ID card or any other product. Every technical and non-technical person should be able to visually identify the difference between a validated and invalid product. It is not possible for every person to check the security strength of an item where evaluation involves a series of steps. To overcome this issue, cybersecurity label can be used to indicate a properly validated product. For instances, Finland became the first country in Europe to initiate the cybersecurity label for smart devices based on EN 303 645[11]. Recently, ECSO introduced a label called Cybersecurity Made in Europe to indicate that the application or product has been developed by a European company or organization[12]. Their intention for issuing this label is to

[11]https://www.traficom.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label

[12]https://ecs-org.eu/working-groups/cybersecurity-made-in-europe-label

broaden the European market by verifying the geo-location of the target company and not for assessing the security intensity of a product. In the ECSO meta-scheme approach [16], the cybersecurity label is represented using the radar diagrams and in the ARMOUR methodology [6], QR diagrams based on the scenarios are used to represent the security strength. We use cybersecurity label similar to the ARMOUR methodology in the context of our case study. We chose this because it helps in representing the certified product as well as the security level of the security properties. Our integrated approach allows the vendors to decide whether to print the label on the certified target.

2.7.3 Assurance Level

In general, assurance is a way to ensure that the product is in compliance with the baseline security requirements through evaluation and the identified vulnerabilities are patched [4]. All certification based on the CC certification scheme ensures the assurance level through Evaluation Assurance Level (from EAL1 to EAL7) based on the system level that was tested. Similarly, the ECSO meta-scheme and the EUCC define that assurance level can be declared based on control assessment [16, 20]. For instance, in the ECSO meta-scheme, the level is represented as base (entry, basic) and advanced (enhanced basic, moderate and high) based on the type of penetration testing and assessment body. Hence in the thesis, we represent the assurance level as basic, substantial and high based on the type of penetration testing carried out on the target. The assessment body should be an accredited third-party. These are discussed more in Section 3.5.

2.7.4 Monitoring

Monitoring is defined as gathering and analyzing the information with the help of continuous monitoring to make a decision in case of exceptions or incidents [42]. The monitoring of the product (ID card chip) must ensure that certificates and products are valid to use. The process ensures that every component in the system meets the security requirements all the time. In this thesis, continuous monitoring (CM) of the chip is defined as in NIST SP 800-137 (Information Security Continuous Monitoring) [38] in compliance with the EUCC [20] rules.

2.7.5 Re-certification

Re-certification can be either periodic or necessary because of the occurrence of some modifications. With continuous monitoring, we can detect if a change or update has been carried out on the target. In these cases, it is necessary to repeat the certification process for either the whole system or a particular

component depending on the change that has been made. For instance, there are numerous certifications to ensure the knowledge and competence of a person. These certificates expire after a certain amount of time. To ensure the candidate is aware of the latest technologies and processes, he or she has to periodically retake the certification test to prove their knowledge. Similarly, the ID card is valid for a certain amount of time and has to be re-certified periodically. Also, re-certification can be triggered for the following reasons or situations:

- when a feature is newly added,
- when there is an update or modification in a feature,
- when there was an attack on the chip,
- when a zero-day vulnerability has been found,
- when the certificates or validity of the card is expired (may be just repeating the previous evaluation, if the mentioned situations are not met),
- when there is a major change in the requirements of the ID card.

We define re-certification based on the modular and incremental certification approach [22] developed by the Industrial Avionics Working Group (IAWG, an industrial consortium). If the listed situations affect the functionalities of the entire chip, then a complete re-assessment of the chip is required. Otherwise, the specified components can be re-certified based on the concept of incremental certification (Section 3.7).

2.8 Summary

We present an integrated approach for the process of certifying and re-certifying based on the Estonian ID card chip. The integrated approach is composed of solutions from the ECSO meta-scheme, the ARMOUR methodology and the NIST SP 800-137. We integrated the solutions in such a way that they complement each other at different steps. The ECSO meta-scheme allows the integration of certification schemes or standards. The ARMOUR methodology supports our integrated approach in establishing the context, testing and communicating the result processes. We selected predefined threats or vulnerabilities from literature and NIST Vulnerability Database (vulnerability scanning is also performed). These vulnerabilities are tested against the SUT by ITSEF based on model-based penetration testing. NIST SP 800-137 supports the continuous monitoring for patches or updates. Finally, the cost and time taken for re-certification are reduced by using incremental certification.

3 Integrated Approach

3.1 Overview

We developed this integrated approach in compliance with the guidelines mentioned in EUCC [20]. Before beginning the chip certification or re-certification process, there are certain terms and conditions that are required to be accepted by the parties (IDEMIA and SK Id Solutions) involved. To establish this mutual recognition, a Mutual Recognition Agreement (MRA) is established between the participants. From EUCC, the thesis adopts the terms and conditions which represent the rules and constraints for the chip certification or re-certification. Once all the conditions are declared in the MRA and is digitally signed by the participants involved, chip certification begins.

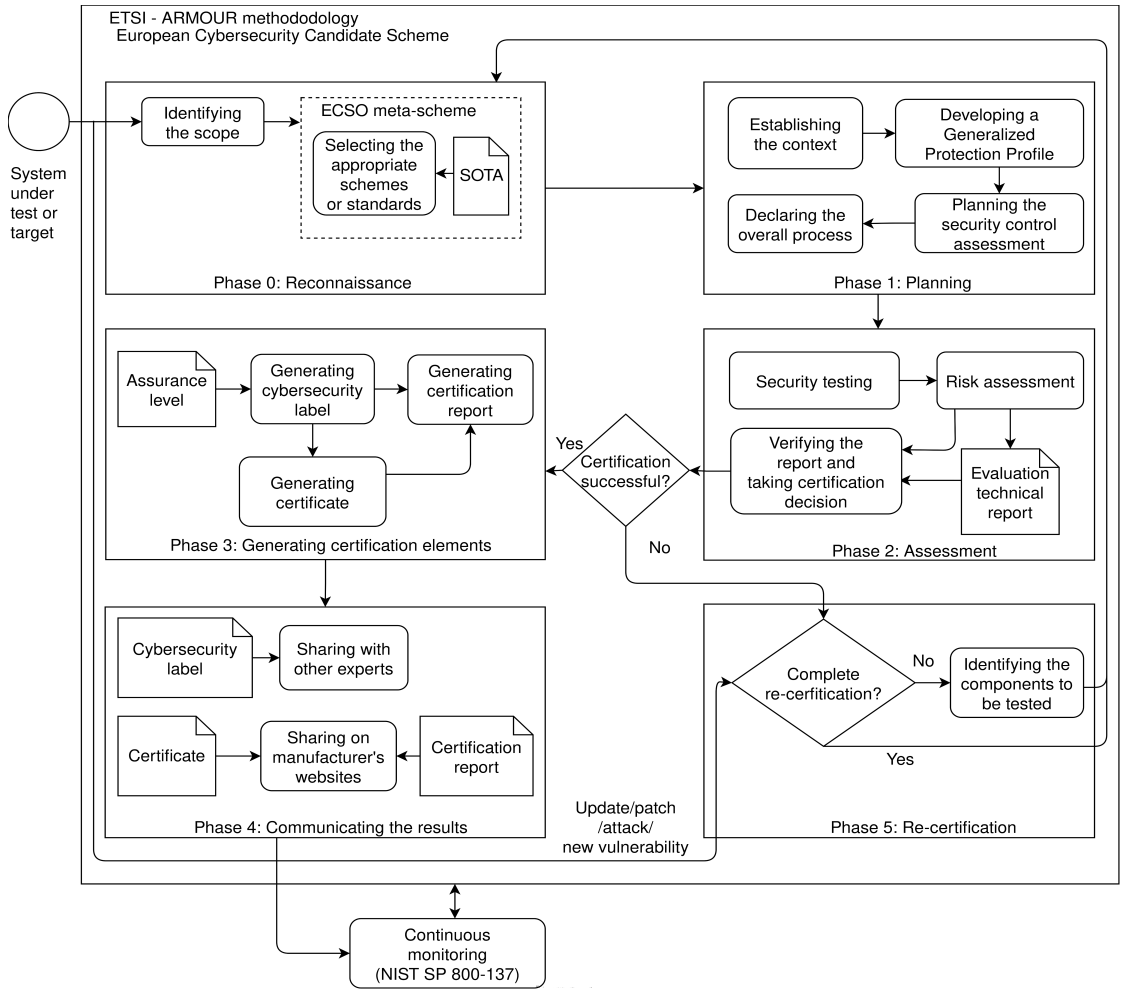

Figure 2. Overview of the chip certification and re-certification.

Figure 2 gives an overview of the certification and re-certification process for the ID card chip. We developed this approach by adopting and integrating required processes from the ARMOUR methodology (Section 2.2) and the ECSO meta-scheme (Section 2.4). We have divided our integrated approach to phases based on the ARMOUR methodology [6], phase 0 (reconnaissance), phase 1 (planning), phase 2 (assessments), phase 3 (generating certification elements), phase 4 (communicating the results), phase 5 (re-certification) and finally, monitoring process.

3.2 Phase 0: Reconnaissance

In this phase, the expert group (EG) gather necessary technical and non-technical information about the system under testing (SUT). For this thesis, the EG is composed the author and their supervisors. We developed Table 2 to represent the mapping of selected threats to the security properties based on the features of the chip.

Table 2. Selected threats and its security properties.

Threats	**Associated Security Property or Vulnerability**	**Source**
When the keys are easily factorizable, computing the private keys through timing side channels	Insecure cryptography	literature
Cryptographic suite – weaker 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 authorization	NIST Vulnerability Database
Spoofing due to the usage of weak pseudorandom number generator	Lack of authentication	NIST Vulnerability Database

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. We have filtered the threats associated with the features of the chip from the sources: the NIST Vulnerability Database and literature (Section 2.1.2). We 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 [20] for the scheme selection from the ECSO State Of The Art Syllabus (SOTA) [18]. 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 [2] and the conditions are specified in the MRA. As mentioned in Section 2.5.1, we decided to integrate the ISO/IEC 19790:2012 standard [26] to the Common Criteria (CC). Note that vendors are allowed to decide whether their product should be certified against national or international scheme or standard.

The EG integrates the schemes based on common language from the ECSO meta-scheme (Section 2.4) that is done in the planning phase (Section 3.3). The EG is also responsible for generating the rules of engagement (ROE) based on the template from NIST SP 800-115 [37]. It contains information like the point of contact, constraints, scope. This ROE is developed for the IT Security Evaluation Facilities (ITSEF) who has to follow these rules during the assessment. The process of listing the ROE is not included in the scope of this thesis. In addition, the EG declares the privacy policies that are to be maintained by ITSEF.

3.3 Phase 1: Planning

3.3.1 Context Establishment

In the planning phase, the EG establishes the context [6] defining the scope and purpose of the target. In this process, the EG analyzes the chip requirements and functionalities in terms of appropriate security properties, business processes, working environment, related laws. As a result of context establishment, the EG derives different profiles with unique names [6]. 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 (Section 3.4.2). With the help of context establishment, the EG can also develop safety cases (SC) required for incremental re-certification (discussed in Section 3.7).

In our integrated approach, the chip is allowed to certify 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 [3] and Common Criteria PPs for secure signature creation device [8]. 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. Every PP or GPP is required to possess the following.

- The security problem definition based on threats or vulnerabilities, assets, constraints and assumptions for the chip (target),
- Security objectives based on problem definition with respect to the considerations of EUCC [20],
- Security services and features based on the objectives and chip functionalities,
- Instantiation levels. This contains schemes selected, list of profiles created, acceptable risk levels and evaluation steps.

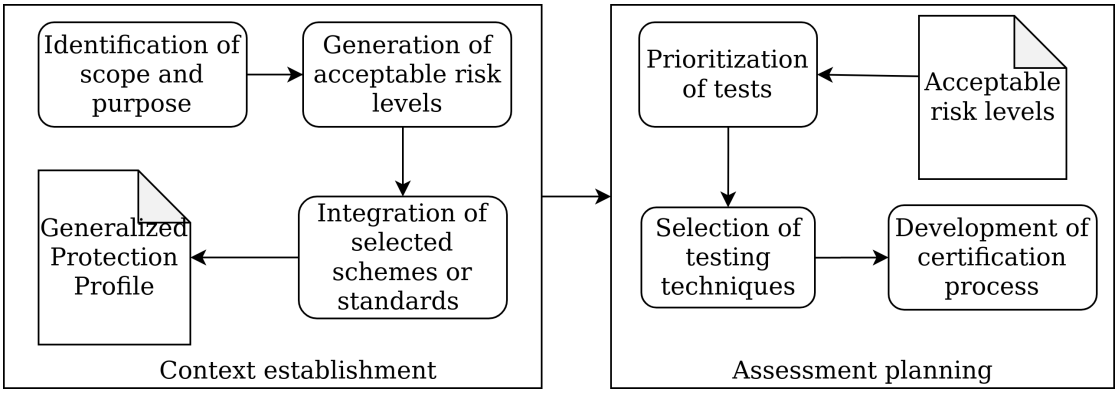

Figure 3. Planning phase.

We developed Figure 3 to represent the activities involved in the planning phase. As mentioned in EUCC [20] and CC [18], the developed GPP is evaluated by an accredited ITSEF. It is sufficient [20] to validate GPP and security target (ST) against APE criteria and ASE criteria respectively from the CC (Part-3) [13]. On a positive evaluation result, a unique ID must be provided to the evaluated

GPP. This evaluation is to ensure that every GPP complies with the requirements of CC though they are developed based on more than one scheme or standard. If the evaluation is unsuccessful, the EG is required to carry out appropriate changes on the GPP or ST. If the vendor or manufacturer prefers, a certificate can be generated for the (positively) GPP evaluated. The format and content for this certificate should be declared based on the EUCC (not covered in the scope of this thesis). 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 [20]. This supplementary cybersecurity information is further discussed in Section 3.6. Though the GPP are subjected to changes, they do not necessarily require monitoring measures.

Based on the information gathered, a test plan is created, where testing techniques, process flow, and testing priorities for the remaining certification and re-certification stages are declared. Note that acceptable risk levels (for each profile) can be reused during a periodic re-certification process assuming that there were no attacks or no updates have been made to the chip components. Otherwise, the process should restart from Phase 0.

3.3.2 Assessment Planning

In this thesis, the approval or denial of certification is decided based on the assessment results against the threats from Table 2. As the EG selected the certification scheme and standard for SUT evaluation in Phase 0, assessment activities shall be planned now. Risk analysis of each threat could help in determining acceptable levels that are specific to each profile. Based on these acceptable risk levels, the tests are prioritized and executed accordingly. These results can be reused until the conditions mentioned in Section 2.7.5 are not met. Based on ARMOUR methodology [6], the following activities are carried out in assessment planning,

1. Prioritizing the tests for the vulnerabilities based on the acceptable risk levels,

2. Selecting the testing techniques and risk assessment approach,

3. Developing an overall certification plan or process.

The testing stage decides the assurance levels of the certification. Hence dedicated security testing activities are required to provide high assurance. The testing techniques have to be selected by the EG and it is possible to use more than one testing technique (Section 2.6.2). Thus, we selected model-based testing

(MBT) and penetration testing for vulnerability exploitation of the chip, where each of the testing techniques has its specific usage. The chip manufacturer decides whether ITSEF has to carry out black-box testing or gray-box testing or white-box testing (Section 2.6.2). In addition, the EG is responsible to decide upon the risk assessment approach. In this thesis, we are using the Common Vulnerability Scoring System to identify the risk levels for the exploitable vulnerabilities. As mentioned in Section 2.6.1, this thesis does not consider self-assessment conformity as an accredited assessment. Hence 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 (like testing technique, ITSEF). This plan in compliance with the responsibilities of CC and ISO/IEC 19790. The detailed explanation of the chip assessments and their responsibilities are mentioned in Phase 2.

Overall Process. 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. Besides, where applicable, the evaluator must be supplied with all the necessary and appropriate information during the evaluation of the chip. We highly recommend to share or exchange information based on the privacy policies from EUCC [20]. The supporting documents that are used by the evaluator during the certification and re-certification processes are mentioned in evaluation technical report (ETR) and the certification report [20]. The company IDEMIA is certified with Level 1 and Level 2 of ISO/IEC 30107-3 [28] by iBeta[13]. SK ID Solutions is responsible for certificate management and is ISO/IEC 27001 certified [27].

We have defined the following overall chip evaluation process based on the CC certification scheme [18] and meta-scheme [16].

1. A GPP is created based on the chip context which is in compliance with the CC and ISO/IEC 19790 (Section 3.3.1). 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.

[13]https://www.ibeta.com/biometric-testing/

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).

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 authorizing scheme[14] (CAS) is responsible for verifying 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 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 researchers and experts. If the certificate has been revoked, results are communicated and re-certification process shall proceed. The process of re-certification is discussed in Section 3.7.

3.4 Phase 2: Assessment

Phase 2 is one of the most important steps of certification or re-certification, as it has a direct impact on the certification decision (Section 3.4.3) through testing and risk assessment. ITSEF or tester is responsible for executing the testing and risk analysis process for 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 has to be carried out but not the procedure or steps on how to accomplish them. Hence we analyzed various testing methods and risk assessment approaches for our integrated approach to carry out the target evaluation. We developed Figure 4 based on [6] to explain the assessment phase of the chip.

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

3.4.1 Model-Based Penetration Testing

Test case generation. In this thesis, ITSEF uses MBT to generate the test cases for the penetration testing scenarios using the tool called CertifyIt [30] 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. We developed Figure 4 to represent the assessment activities involved.

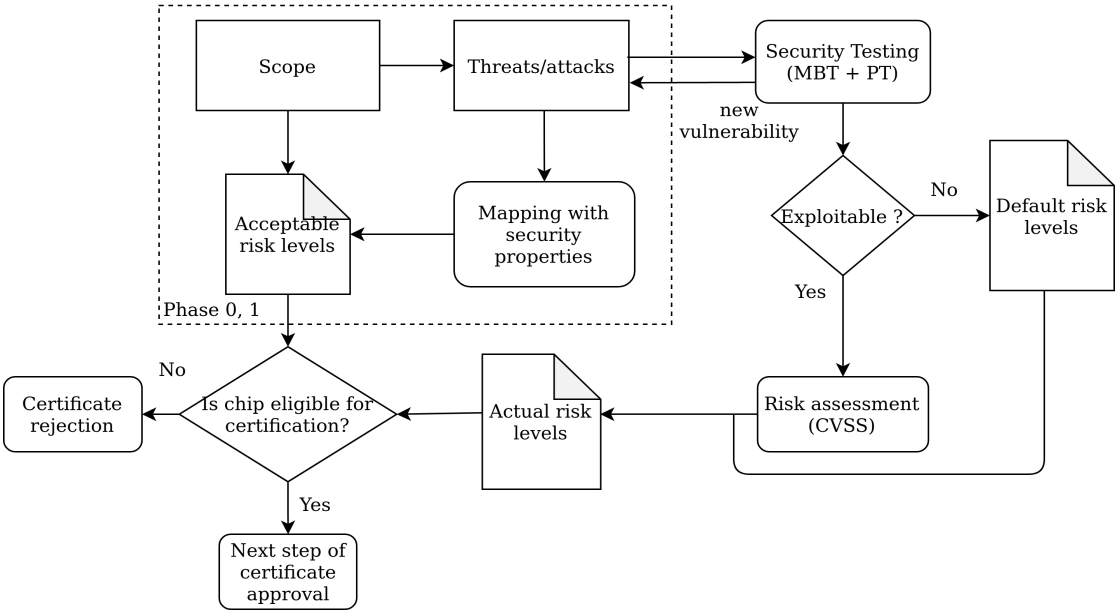

Figure 4. Testing process for the ID card chip.

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 [47] for the test execution step. PTES provides a common language for carrying out penetration testing and reporting all its results. In this thesis, we assume that ITSEF carries out penetration testing on the test cases generated from the test case generation step based on the 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 4) 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.

3.4.2 Risk Assessment

CC does not include risk assessment as on the responsibilities. However, to address and prioritize the vulnerabilities or threats, our integrated approach includes risk assessment. From the testing process vulnerabilities that can be exploited are filtered. These vulnerabilities are given as input to the risk analysis process to determine the actual risk level with respect to the context or profile. This thesis makes use of the Common Vulnerability Scoring System (CVSS) to compute the risk level. We developed Table 3 to represent the risk levels based on CVSS v3.1 [23].

Table 3. Risk level.

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

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 intervals shown in Table 3. There are some exceptional cases where the vulnerabilities are provided with the default risk level. Based on ARMOUR methodology [6], vulnerabilities

with no protective measures are classified as critical risk and the vulnerabilities that cannot be exploited at present are classified with the low risk level. Our integrated approach 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. This can allow ITSEF to automate the estimation of risk scores partially. Risk mitigation suggestions can be mentioned by ITSEF or the pentesters which could be useful for the EG to prepare the mitigation activities. This risk treatment is not in the scope of this thesis.

All the necessary information from the testing and risk assessment of the chip are generated as evaluation technical report (ETR). ETR should contain sufficient information about the assessment which will be validated by the certificate authorizing scheme. For instance, 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 testings. Looking at the aspects of privacy, ETR or other sensitive information of chip assessment (results of risk assessment, penetration testing) must be shared only with the chip manufacturer or manufacturer approved person. For instance, if the details of the exploitable vulnerability are disclosed, it could pose a huge threat to the manufacturer.

3.4.3 Certification Decision

Based on the outcome of the assessment phase, the certificate authorizing 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 risk levels obtained from the assessment phase (Section 3.4.2) are compared with the acceptable risk levels generated by the EG in the planning phase (Section 3.3). The profile comparison is based on the comparison described in [6]. Every profile whose acceptable risk level matches the actual risk level is considered as a profile fulfilled. Hence it is possible to avoid testing the particular vulnerability against the specific context unless the situations like changes, attacks on the target have occurred (Section 2.7.5).

When all the profiles are fulfilled and selected, then the chip is considered to be eligible for certification and proceeds to the next phase. In addition to the profile fulfillment, evidence for performed evaluation (ETR) must be provided to the certificate authoring scheme [20]. The certificate authorizing scheme is also responsible to make sure that the Mutual Recognition Agreement (MRA) is not violated and the rules of engagement mentioned in the MRA are satisfied. When the certain profile is not fulfilled, then the identified threats are prioritized for re-certification (after the mitigation) based on the risk level. We developed Table

4 to represent the certificate decisions based on the assessment results and the evidence provided.

Table 4. Certification decisions.

Situations	**Decision**
The certified ID card chip meets the requirement criteria	Issue the certificate
The certificate of the ID card chip expired, no updates or modifications or attack happened 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 attack happened(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 happened 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 not requested for the certificate maintenance	Archive the certificate
The certified chip components had updates or modifications or attack happened(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	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	Withdraw the certificate

3.5 Phase 3: Generating Certification Elements

For the purpose of simplicity, we are using the type of penetration testing that carried out on the chip to represent the assurance level. The penetration testing type decides the assessment depth based on the information shared with ITSEF for evaluation (Section 2.6.2). 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. We developed Table 5 to represent the assurance levels.

Table 5. Assurance level with respect to penetration testing type.

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

3.5.1 Cybersecurity Label

As discussed in Section (2.7.2), the cybersecurity label for the ID card chip should be generated only when the certification is completed successfully. It is valid only for a certain period of time (based on certification validity). If the assessment criteria is not fulfilled, use of the cybersecurity label on the chip is prohibited [20]. Such practices have legal implications which are not in the scope of this thesis. Based on the ARMOUR methodology [6], the label should contain the following information.

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

Our integrated approach allows the chip manufacturers to generate a multi-dimensional label to represent the level of different security properties [6]. This cybersecurity label is shared with experts at Phase 4 (communicating the results) for consulting the target evaluation. This label is dynamic which varies based on the certification results of the chip. But it is not mandatory to display the label on the certified product. The manufacturer is responsible for deciding whether to add the label on the certified product.

3.5.2 Certification Report

A certification report is created to address all the information about the chip certification process. The report is issued based on evaluation technical report (ETR) by the certificate issuer. The report can be published on the CC portal or vendor's manufacturer based on the availability conditions discussed in Section 3.6. This report should follow the content and format based on the EUCC [20]. This leads to the creation of a unified report format for all vendors. We propose the content for a certification report based on EUCC [20] as follows,

1. Executive summary, an overview of the assessment results.
2. Target details, both technical and non-technical information.
3. Scope and assumptions, environmental details, limitations in evaluating the target like the threats that we are considering in assessing the target.
4. Security policies, rules or constraints that ITSEF should comply with.
5. Certification schemes or standards, information about the schemes and standards involved in certifying the target.
6. Supplementary cybersecurity information, all the information is added with respect to CSA Article 55 [2]).
7. Conformity assessment body, ITSEF details.
8. Evaluation results, details about testing techniques, tools used and assessment results.
9. Certificate details, contains unique ID, issuance date, validity.
10. Summary, includes the certification decision, description of security level of the target.
11. Cybersecurity label, generated label can be added in the report (Section 3.5.1).
12. Bibliography, references to the supporting documents like technical documentation of the target.

If every certification report contained the listed information in a structured format, it would allow for an easy overview and comparison of the certificates. A reference to this certification report can be added to the certificate. In addition, vendors can generate the European Cyber Security Certificate report [16] or any other summarized report based on the certification report, if required.

3.5.3 Certificate

Our integrated approach uses content and format from the EUCC [20] for generating the certificates for the certified chip. These certificates should contain the specified information in the following format,

1. An ID that is unique to the certified target,
2. Information about the certified target
   (a) Name of the certified product,
   (b) Type and version (if applicable),
   (c) Manufacturer,
   (d) Link to access Supplementary security information of the chip based on CSA Article 55 [2].
3. Technical information of the certified target
   (a) Authority Name and contact information that issued the certification,
   (b) Accredited third party lab information who performed the testing and risk assessment, if it is different from the authority body,
   (c) Certification standards or schemes involved and its version,
   (d) Assurance level: basic or substantial or high,
   (e) Reference to certification report,
   (f) Reference to GPP of the certified target,
   (g) Reference to certification schemes or standards involved,
   (h) Date of issuance and date of expiration.
4. Cybersecurity label.

These details should be present in the chip certificate and the format is applicable to all the ICT product certificates. Our approach recommends generating this certificate in English when shared publicly such as vendor's website, CC portal. If the vendor prefers, they can generate the report in their local language (along with a courtesy translation in English) and share it on their website. In addition, it is the responsibility of the issuer of the certificate to provide a guideline for the users in accessing the relevant information about the chip certification using the unique ID of the certified target. The certificate issuer may create a standardized format for the guidance or rules (may refer from the ENISA guidance, if required) and use the format for all the products with an automated script instead of creating individual guidelines for each product. This process is not in the scope of this thesis.

3.6 Phase 4: Communicating the Results

In this phase, we can communicate the chip evaluation results with experts or researchers through the cybersecurity label. Based on the conditions specified in [20], information like feedback, suggestion about the PPs is shared and received with other experts. The certificates generated for the certified chips are valid for a maximum of five years from the date of certificate issuance [20]. This initial period of validity can be extended if none of the conditions mentioned in Section 2.7.5 has occurred in those five years (ie., that the certified ID card chip meets its required security baselines). On the other hand, if any one of those conditions occurred before the expiration of the chip certificate, the validity ends (as validity may require re-certification).

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 [2]. 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 issuer can also refer to the ENISA guidance (if required).

The published information should be available only 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 again made available for five years from the newly released expiration date. The information required by the ITSEF and the chip manufacturer for the conformity assessment like assessment samples or any sensitive data should be shared only upon request and the shared data must be stored securely. The conditions for sharing and publishing should be mentioned in the Mutual Recognition Agreement (MRA) under appropriate sections [20].

3.7 Phase 5: Re-certification

Incremental Certification. Incremental certification is the process of identifying and evaluating the parts of the chip that need to be re-certified instead of evaluating the whole chip. Lack of certification support for the life-cycle of the product and the high cost are the issues considered by our integrated approach. These two considerations are taken from an ENISA survey [19]. Generally, the re-certification of the chip or any product has a high cost and is time-consuming. Hence with the help of continuous monitoring, we can identify the changes and re-certify only the necessary parts. This can reduce the impact on other business processes, effort and overall cost. This is possible only when 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[15] (SC) represents proof or evidence ensuring that a system is safe to use in the given environment through a set of organized arguments. As mentioned in Section 3.3, 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, our integrated approach helps in certifying only specific component that requires re-certification instead of re-certifying the whole chip (unless required). Thus, our integrated approach can reduce the cost and effort required to re-certify the chip. We have defined the following steps for the expert group by adopting terms and processes like SC, dependencies, relationships, safety argument from [22] and integrated them with our approach to achieve modular and incremental certification.

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

Step 2. Initially, the EG identifies why, how and what has been changed. Then the EG compares the change scenario happened on the chip with various scenarios listed in Section 2.7.5). 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 the whole re-assessment. 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. Dependency-guarantee contract (DGC) is identified by the EG if required. The DGC defines the relationship between the software elements. Correctness and completeness of the DGR and the DGC decide the validity of the safety argument. Hence manual generation of the DGR is suggested for a higher assurance level.

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 chip processes (entire system). These SA modules are integrated 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

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

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 (as discussed in Section 3.3).

Step 8. All the requirements from step 1-7 are accomplished and given as input to the planning phase to update the Generalized Protection Profile and the security target. Also compliance is verified against CC requirements (discussed in Section 3.3). All the previous assessment reports and required documents can be shared with ITSEF under the EUCC [20] 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 authorizing scheme decides whether to provide a certificate to the chip. Finally, the results are shared and a common unified report is generated. These are covered in Phases 2, 3 and 4 of our integrated approach. Note that if more than one change scenario occurred, scenarios are prioritized based on the significance of the scenario or impact that can be caused by the vulnerability if exploited.

3.8 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 (Section 2.7.4) 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 [20]. As there are various advantages (Section 2.7.4), our integrated approach includes continuous monitoring and generation of status reports. Based on the NIST SP 800-137 [38], we define the monitoring process for our integrated approach as follows.

Step 1. We need to define an Information Security Continuous Monitoring (ISCM) strategy with respect to context establishment and to allow the reuse of processes or information in future. We need to provide required information about the chip (target) for the strategy to look through, where applicable. 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. For instance, a repository can be maintained where all the information is stored or links to public vulnerability databases (like NIST Vulnerability Database) should be provided to look for the required information.

Step 2. In the second step, we need to determine the metrics and set the frequencies for monitoring and reporting. A metric is an organized information developed to support risk management decisions or helpful in generating status reports. The metrics can be derived from assessment result status reports, predefined vulnerabilities (Table 2) or other security information gathered by the EG in Phases 0 and 1 (through the manual procedure). The frequency of metric determination should be flexible. This flexibility varies based on requirements and significance of the metric. Finally, we develop a technical architecture which is composed of five steps. This architecture defines how the information from step 1 is collected, how that information is stored, how the information is analyzed and accessed for response and how the status reports are generated. In addition, this architecture helps in understanding the overall workflow of monitoring and its interoperability. This technical architecture is not defined in the scope of the thesis.

Step 3. In this step, we implement the technical architecture (five steps) and we initiate the monitoring. Our integrated approach is allowed to use any relevant tools during data collection or analysis if required. Assessments should be conducted and related information like evaluation technical report, ITSEF details are collected and stored in the repository. At this point, for instance, we can set the frequency for the generation of a status report about the assessment. This status report can contain information about the assessment completion, assessment compliance with EUCC, conflicts (if occurred). Such a report can be helpful for the EG to ensure that the chip evaluation meets the compliance requirements.

Step 4. The monitoring results (metric), status reports and other collected information are analyzed and verified by the EG manually at periodic intervals. For instance, if a component requires mitigation actions, the EG is responsible to verify whether appropriate actions are carried by the corresponding team out at a given time through the status report. The EG reports all the findings in a document after analyzing and the report is stored in the repository.

Step 5. All the findings made by the EG are responded with appropriate decisions by the vendor. For instance, when any chip profile (Section 3.3) is not fulfilled, appropriate measures are taken by the mitigation team to mitigate the

corresponding exploitable vulnerability. Also, if any situation mentioned in Section 2.7.5 is detected on the certified chip, then the chip is subjected to re-certification. Status reports should be generated when the appropriate response decisions are taken.

Step 6. If required, based on the findings and responses, we can refine the ISCM strategy in terms of visibility of information, frequency of monitoring or reporting and metric determination. These modifications are made based on the chip certification requirements and enabled monitoring features.

We can required policies or procedures to facilitate the steps 1-6 [38] (not in the scope of this thesis). The CM of our integrated approach is responsible for fulfilling certain tasks, compliance requirements and conditions. We define the following (but not limited to) responsibilities and rules based on the EUCC [20]. These can be accomplished by monitoring our integrated approach and the responsibilities are,

- To ensure that the scope and target information are clearly defined,
- To detect if a process, rule, condition or decision is not in compliance with the rules and constraints mentioned by the target manufacturer,
- To detect if the situations discussed in Section 2.7.5 occurred on the certified target (for re-assessment),
- To ensure that appropriate decisions or actions are taken based on the findings and associated impact,
- To ensure that ITSEF is provided with sufficient and valid information by the target manufacturer,
- To ensure that ITSEF follows the rules of engagement generated by the EG and ITSEF provides proper and valid evidence,
- To ensure that certification elements including the cybersecurity label (Section 3.5.1), the certification report (Section 3.5.2) and the certificate (Section 3.5.3) are generated and maintained as described in their respective sections,
- To ensure that certificate decisions of the evaluated target are taken based on Table 4,
- To keep track of the public vulnerability databases (like NIST Vulnerability Database) for new vulnerabilities that are relevant to the target,

- To ensure that rules for validity and availability of information mentioned in Section 3.6 are followed by the target manufacturer,
- To ensure that the MRA is not violated.

These conditions are considered to be the most significant as they can have a high impact on the certification activities of the chip. When any deviations are found, appropriate decisions or actions must be taken based on the MRA (not in the scope of this thesis). When an organization is certifying more than one item, to monitor a particular certified chip (or any other product), filtration is done based on the manufacturer or product or ITSEF. In these cases, for instance, predefined keywords can help refine the results.

To ease the process of remediation, roles and responsibilities of the person who is required to complete the task can be predefined. The guidelines for defining the roles and specifications can be taken from NISTIR [43]. With the help of monitoring and role definitions, the assignment of remediation measures can be automated. This process is not in the scope of this thesis. Once the chip manufacturer (vendor) carries out all the updates or remediation, the process of notifying ITSEF and initiating the re-certification of the chip can be automated. To achieve this, we need continuous monitoring so that we can keep track of all actions and also the EG should declare the components to be assessed. Then the approved ITSEF is notified to proceed with Phase 2 (assessment phase).

4 Research Validation

To validate that our integrated approach (based on the ECSO meta-scheme, the ARMOUR methodology and the NIST SP 800-137) satisfies the research objectives, we make use of face validity. We selected 3 validators who are interested and have knowledge about certification and re-certification of a product. We have developed a set of questions for an interview with each validator. The questions are the same for all validators. Hence validators are allowed to make exceptions if they find a question from an unfamiliar topic. The following sections show the questions and the answers made by each validator along with the modifications made in our integrated approach.

4.1 Interview Questions

1. How familiar are you with the certification and re-certification processes?
2. Are the standards used in our integrated approach nationally or internationally recognizable?
3. Do the selected standards appropriate to the chip functionalities?
4. Would you like to suggest/include any other existing Protection Profile?
5. Apart from the semi-automation activities mentioned, can you think of any other possibilities for a process that can be automated in our integrated approach?
6. Does our integrated approach satisfy the requirements mentioned in European Cybersecurity Candidate Scheme (EUCC)?
7. Does our integrated approach answer to the research questions?
8. Would you like to suggest any tools or ideas that could help automate/refine any actions in the integrated approach?
9. If our integrated approach is practically implemented, what could be the advantages and disadvantages?
10. Would you like to suggest any section in our integrated approach that requires more clarifications/explanations/modifications?
11. What is your overall feedback?

4.2 First Validation

After the 80% completion of the research work, the first validation interview took place. Validator 1 has experience in working with split-key certification, helped in preparing related documentation, helped in proof-reading the ID card related research papers and participated in various research on European projects. As the validator was not familiar with the EUCC [20], the validator was not able to provide feedback about the EUCC requirements accomplished in our integrated approach. The validator suggested the author to have hands-on experience with the related tools and techniques to decide on how far automation can realistically be achieved. On considering the issue of transparency, we made it mandatory in our integrated approach to print the security label on the certified product. But after the first validation, our integrated approach allows the vendors to decide upon the display of label on the certified product. On the other hand, the Cybersecurity Act [2] highly recommends the usage of a cybersecurity label. Also, this label can simply be accommodated with all required technical information, as mentioned in Section 3.5.1. Thus, our integrated approach uses the label to communicate with the other researchers or experts in the communicating the results phase (Section 3.6) [35]. The validator mentioned that addressing side-channel attacks on the chip is significant. Also, the validator suggested addressing the physical attacks that are possible on the chip (which we consider as future work).

4.3 Second Validation

After completing the research work, the second validation interview took place. Validator 2 has a great role in developing the ARMOUR methodology [35] and most of their projects are based on certification and re-certification. In terms of certification standards or schemes, the validator addressed that it is good to have the Common Criteria as the base scheme for certification as it is an internationally recognized generic scheme. But the validator is not much familiar with the chip requirements and its life-cycle. Hence the validator cannot confirm whether the standard (ISO/IEC 19790) that is selected for integration is the best. The validator suggested selecting the schemes or standards from the ECSO SOTA to ensure that they are valid and actually exist. In addition, the validator could not suggest Protection Profiles that can be considered in the chip certification, as it may require detailed analysis of the chip requirements. The validator addressed that the usage of EUCC [20] could make our integrated approach to be standardized, cost-effective and increases the possibility of automation. Specifically, the validator supported the idea of using the same content and format (from EUCC [20]) for the certification report leading to a unified document for all vendors. The validator mentioned that the specified research questions are answered in our integrated

approach.

In terms of semi-automation, the validator prefers the context establishment, planning and model design to be manual as it requires understanding and experience to make better decisions. The validator suggested using penetration testing tools where applicable to automate certain processes. In addition, the validator asked the author to look for the possibilities to partially automate the risk assessment and risk treatment steps (like usage of tools). Initially, we preferred the risk assessment step to be a manual process. But after the validator's suggestion, our integrated approach allows ITSEF (testing laboratory) to make use of accredited tools for partially automating the risk estimation, if applicable. The partial automation of risk treatment is considered as the future work using NISTIR [43]. In terms of refinement or future work, the validator mentioned that our integrated approach could be more beneficial if it includes the aspects of privacy and supports complex systems through the analysis of vulnerability or risk dependencies. In terms of benefits, the validator mentioned that there are some disadvantages with the CertifyIt tool with respect to configuring. The validator also mentioned that it is still the best tool for model-based testing so far. The validator commented that model-based testing could be complex to implement at the beginning. But it can be highly helpful in partial automation of test generation, once implemented properly.

4.4 Third Validation

After completing the changes mentioned by the second validator, we had our third validation. Validator 3 has experience in working with the product certification through one of his projects. In terms of standards or schemes, the validator prefers to use schemes that are internationally recognizable rather than nationally to avoid compliance issues. However, we are allowing the manufacturers to decide between the national or international standards. The validator is aware of the EUCC [20] and agrees that our integrated approach is in compliance with those guidelines where applicable. The validator prefers to use the existing PPs rather than creating a new PP which might increase the workload. In terms of semi-automation, the validator prefers the risk assessment to be a manual process, instead of using tools.

The validator asked about the benefits of using penetration testing as the testing technique. The testing process in our integrated approach is composed of two techniques to complement each other (model-based penetration testing). We chose model-based testing so that the generated test cases can be reused for the re-certification process. The reason for choosing penetration testing is to simulate real-world attacks. The validator commented that combining standards might not improve the results. As mentioned, a single scheme or standard cannot fulfill all

the requirements of a product. Hence our idea from the ECSO meta-scheme is to integrate the requirements of the selected schemes or standards through the Generalized Protection Profile. This profile can be used to evaluate the target. The evaluation against the requirements of more than one standard or scheme can increase the level of confidence or rigorous level during the testing [16].

As overall feedback, the validator mentioned that practical implementation of our integrated approach could be difficult, as it considers solutions from different organizations and requires high knowledge and experience. The validator suggested reducing the size of Section 2 which deals with the background information. In addition, the validator mentioned stating the author's contribution very clearly in the thesis, as there is a lot of information given in our integrated approach. We took these suggestions into account and modified the thesis accordingly.

4.5 Summary

We have modified our integrated approach as suggested by the validators or addressed their suggestions as future work in the thesis. Since our integrated approach is defined at a theoretical level, we did not perform practical validation using our approach. Thus, the thesis validation is limited to face validity.

5 Conclusion

The outcome of this research work is an integrated approach based on three different solutions from three different organizations (ETSI, ECSO and NIST). Our integrated approach involves the certification and re-certification process based on the integrated circuit case study. The goal of our approach is to integrate the existing or refined schemes and standards to increase the assurance of target evaluation. The ARMOUR methodology and the ECSO meta-scheme complement each other in our approach and thus, we could overcome their drawbacks. In order to define a standardized approach, we follow the EUCC guidelines throughout the process. In addition, our integrated approach deals with increasing the transparency, lowering the cost and time consumption of certification and re-certification. The approach has been validated by three different validators through face validity.

5.1 Answers to Research Questions

RQ1: How to define the certification and re-certification of the chip using national or international schemes or standards at minimal time and cost?

RQ1.1: How to describe the testing process?
We are using a combination of model-based testing and penetration testing for the target security testing. The test cases generated from model-based testing are given as input to penetration testing for simulating the real-time attacks. This is discussed in Section 3.4.1.

RQ1.2: How to semi-automate the security control assessment?
We define how to partially automate the testing process of the chip. During penetration testing, IT Security Evaluation Facilities (ITSEF) is allowed to use tools when required. For instance, vulnerability scanners can be used for identifying any existing or new vulnerabilities. The partial automation of risk mitigation is a part of future work. The assessment process is discussed in Section 3.4.

RQ1.3: How to reduce the time and cost taken during re-certification ?
We reduce the cost and time taken for re-certifying a chip through incremental certification. We select certain chip profiles that requires re-certification, instead of re-certifying the whole chip. This is discussed in Section 3.7.

RQ1.4: How to improve the transparency of a properly certified chip?
The transparency of the chip certification is improved in our approach by

declaring a security label for certified chips based on the ARMOUR methodology. This is an optional element based on the vendor's preference. This is discussed in Section 3.5.1.

RQ1.5: How to modify the approach defined in the thesis to support all kinds of products?
The selection of schemes, vulnerabilities and Protection Profiles are the sections that need to be modified appropriately. The expert group is responsible for performing this selection process based on the target functionalities and for integrating that with the base scheme (here, Common Criteria). By performing these modifications, the integrated approach can be used for certifying and re-certifying other items (products, processes, services).

5.2 Future Work

Our integrated approach can be useful for companies or manufacturers who aim to develop a certification framework (from information gathering to the re-certification process) or to certify their product in a standardized manner. To use our integrated approach, one benefits from knowledge of the ARMOUR methodology, the ECSO meta-scheme, the NIST SP 800-137 and incremental certification.

Currently, our integrated approach is limited to the theoretical level and the ID card chip case study. Hence future work involves practical implementation of the proposed approach, certification and re-certification of other ICT products using the proposed methodology. The thesis did not include the process of defining the risk treatment. Guidelines from the NISTIR 8011 [43] can be used to define the risk mitigation steps with partial automation. Another future work would be looking at manufacturing and issuing aspect as well to get an idea of certifying processes and manufacturing. This can help to generalise the approach. To support complex projects, risk dependencies between vulnerabilities and risks can be analyzed in our integrated approach.

References

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

[2] 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 526/2013*. 2019. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj.

[3] Infineon Technologies AG. *Security IC Platform Protection Profile with Augmentation Packages*. 2014. URL: https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf.

[4] Ross Anderson. *Software Engineering v3 - Chapter 28: Assurance and Sustainability*. Wiley, 2020.

[5] Matt Bishop. "About Penetration Testing". In: *IEEE Security & Privacy* 5 (2007), pp. 84–87. DOI: 10.1109/MSP.2007.159.

[6] Dan Bogdanov, Liina Kamm, and Sara Nieves Matheu García. *CyberSec4Europe D3.8 Framework and Toolset for Conformity*. 2020. URL: https://cybersec4europe.eu/wp-content/uploads/2020/03/D3.8-Framework-and-Toolset-for-Conformity-v1.0-Submitted.pdf.

[7] Jordi Cabot and Martin Gogolla. "Object Constraint Language (OCL): A Definitive Guide". In: *Formal Methods for Model-Driven Engineering: 12th International School on Formal Methods for the Design of Computer, Communication, and Software Systems, SFM 2012, Bertinoro, Italy, June 18-23, 2012. Advanced Lectures*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 58–90. DOI: 10.1007/978-3-642-30982-3_3.

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

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

[10] Chen Chen et al. "A systematic review of fuzzing techniques". In: *Computers & Security* 75 (2018), pp. 118–137.

[11] *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model.* 2017. URL: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf.

[12] *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components.* 2017. URL: https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf.

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

[14] Lajos Cseppentő and Zoltan Micskei. "Evaluating code-based test input generator tools". In: *Software Testing, Verification and Reliability* 27 (Feb. 2017), e1627. DOI: 10.1002/stvr.1627.

[15] ECSO. *Challenges of the Industry. Internal document.* 2017.

[16] ECSO. *European Cyber Security Certification, A meta-scheme approach v1.0.* 2017. URL: https://ecs-org.eu/documents/publications/5a3112ec2c891.pdf.

[17] ECSO. *European Cyber Security Certification, Assessment Options.* 2019. URL: https://ecs-org.eu/documents/publications/5ea49d3a940a3.pdf.

[18] ECSO. *State of the Art Syllabus updated.* 2017. URL: https://ecs-org.eu/documents/publications/5a31129ea8e97.pdf.

[19] ENISA. *Considerations on ICT security certification in EU: Survey Report.* 2017. URL: https://www.enisa.europa.eu/publications/certification_survey.

[20] ENISA. *Cybersecurity Certification: EUCC Candidate Scheme.* 2020. URL: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme.

[21] ETSI. *ETSI EG 203 251: Methods for Testing Specification; Risk-based Security Assessment and Testing Methodologies.* 2015. URL: https://www.etsi.org/deliver/etsi_eg/203200_203299/203251/01.01.01_50/eg_203251v010101m.pdf.

[22] J.L. Fenn et al. "The Who, Where, How, Why And When of Modular and Incremental Certification". In: 2nd Institution of Engineering and Technology International Conference on System Safety, Nov. 2007, pp. 135–140. DOI: 10.1049/cp:20070454.

[23] FIRST. *Common Vulnerability Score System (CVSS) v3.1.* 2015. URL: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

[24] ISECOM. *The Open Source Testing Methodology Manual (OSSTMMv3)*. 2010. URL: https://www.isecom.org/OSSTMM.3.pdf.

[25] *ISO 31000:2019 Risk management - Guidelines*. 2018. URL: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en.

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

[27] *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. 2013. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

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

[29] *ISO/IEC/IEEE 29119-1:2013, Software and systems engineering — Software testing — Part 1: Concepts and definitions*. 2013. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:29119:-1:ed-1:v1:en.

[30] Bruno Legeard and Arnaud Bouzy. "Smartesting CertifyIt: Model-Based Testing for Enterprise IT". In: *2013 IEEE Sixth International Conference on Software Testing, Verification and Validation*. 2013, pp. 391–397. DOI: 10.1109/ICST.2013.55.

[31] Wenbin Li, Franck Le Gall, and Naum Spaseski. "A Survey on Model-Based Testing Tools for Test Case Generation". In: Springer International Publishing, Mar. 2017, pp. 77–89. DOI: 10.1007/978-3-319-71734-0_7.

[32] "Chapter One - Security Testing: A Survey". In: ed. by Atif Memon. Vol. 101. Advances in Computers. Elsevier, 2016, pp. 1–51. DOI: https://doi.org/10.1016/bs.adcom.2015.11.003.

[33] MITRE. *Common weakness scoring system (CWSS)*. 2014. URL: https://cwe.mitre.org/cwss/cwss_v1.0.1.html.

[34] Matus Nemec et al. "The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli". In: *24th ACM Conference on Computer and Communications Security (CCS'2017)*. ACM, 2017, pp. 1631–1648.

[35] Sara Nieves Matheu García et al. *Towards a Cybersecurity Certification Framework for the Internet of Things*. 2018. URL: https://www.armour-project.eu/wp-content/uploads/2018/01/white_paper_ARMOUR-IoT-Certification.pdf.

[36] NIST. *FIPS 140-2, Security Requirements for Cryptographic Modules*. 2001. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf.

[37] NIST. *SP 800-115: Technical Guide to Information Security Testing and Assessment*. 2008. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.

[38] NIST. *SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. 2011. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf.

[39] NIST. *SP 800-30, Guide for Conducting Risk Assessments*. 2012. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[40] NIST. *SP 800-53A Rev. 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*. 2014. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.

[41] *NISTIR 7298 Revision 2: Glossary of Key Information Security Terms*. 2013. URL: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

[42] *NISTIR 7756: CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Model*. 2012. URL: https://csrc.nist.gov/csrc/media/publications/nistir/7756/draft/documents/draft-nistir-7756_second-public-draft.pdf.

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

[44] Arnis Parsovs and Danielle Morgan. "Using the Estonian Electronic Identity Card for Authentication to a Machine". In: Springer International Publishing, Nov. 2017, pp. 175–191. DOI: 10.1007/978-3-319-70290-2_11.

[45] Ina Schieferdecker. "Model-Based Fuzz Testing". In: *2012 IEEE Fifth International Conference on Software Testing, Verification and Validation*. 2012, pp. 814–814. DOI: 10.1109/ICST.2012.180.

[46] Ina Schieferdecker. "Model-Based Testing". In: *IEEE Software* 29 (Jan. 2012), pp. 14–18. DOI: 10.1109/MS.2012.13.

[47] The PTES Team. *The Penetration Testing Execution Standard Documentation Release 1.1*. 2017. URL: https://buildmedia.readthedocs.org/media/pdf/pentest-standard/latest/pentest-standard.pdf.

Appendix

I. Licence

Non-exclusive licence to reproduce thesis and make thesis public

I, **Jayavarshini Thirumalai**,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

   reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

   An integrated approach for certification and re-certification based on the case study of an integrated circuit,

   supervised by Dr. Liina Kamm and Mari Seeba.

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Jayavarshini Thirumalai
14/01/2021