EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBERSECURITY CERTIFICATION

EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS

V1.1.1 | MAY 2021

DOCUMENT HISTORY

Date	Version	Modification	Author's comments
13/12/2019	0.1	Creation	
28/02/2020	0.2	Integration of first AHWG outcomes	Editor's note: the current version of the document addresses two types of chapters: -Chapters where sufficient matter has been delivered by the TG (or the ECCG Subgroup) so that ENISA can propose a text -Chapters for which TG (or the ECCG Subgroup) have still to deliver: in that case, expected topics to be addressed are listed *in italic*, in the form of questions (additional topics arising from the TG will be included)
24/04/2020	0.3	Integration of new AHWG outcomes from the 3rd and 4th meetings, and of first mandatory applicable documents	Prepared for the 5th AHWG meeting
18/05/2020	0.4	Integration of new AHWG outcomes from the 5th meeting and directly from TG Rapporteurs outputs	Prepared for the 6th AHWG meeting
25/05/2020	0.5	Integration of new AHWG outcomes from the 6th meeting and directly from TG Rapporteurs outputs	Prepared for the 2nd batch of "closer group" review
02/06/2020	0.6	Integration of AHWG outcomes from the 6th meeting and directly from TG Rapporteurs outputs	Residual chapters included for the 3rd batch of "closer group" review
09/06/2020	0.7	Integration of the comments from the "closer group" review	Prepared for the AHWG review
23/06/2020	0.8	Integration of the comments from the AHWG review and of the annexes	Prepared for presentation to ENISA MT
01/07/2020	1.0	Integration of the last AHWG comments	Prepared for the external consultation in accordance with Article 49.3 of the CSA
07/09/2020	1.1	Update based on the outcome of the external consultation and on ECCG comments	Prepared for submission to the opinion of the ECCG
18/05/2021	1.1.1	Cosmetic changes and update of annex 10 based on its recent evolution within the SOG-IS	Version delivered to the EC as a consolidated candidate scheme

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

To contact the authors, please email certification@enisa.europa.eu.
For media enquiries, please email press@enisa.europa.eu.

AUTHOR

European Union Agency for Cybersecurity (ENISA)

ACKNOWLEDGEMENTS

ENISA thanks the members of the AHWG https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ahWG01/ahwg01_members as well as the representatives from the Accreditation Authorities, Members States and the European Commission who have been supporting ENISA for the establishment of this candidate scheme since November 2019.
ENISA thanks the SOG-IS MRA community https://www.sogis.eu/uk/status_participant_en.html for the possibility to reuse the available documentation into the EUCC scheme.

LEGAL NOTICE

This draft document constitutes a preparatory legal text to be submitted for consultation under article 49 of the Cybersecurity Act (Regulation 2019/881). It represents the preliminary views of ENISA, and may not in any circumstance be regarded as stating of an official position of ENISA or the Commission. It does not constitute a legal act of ENISA or Commission or the ENISA or Commission bodies. No rights can be derived from it.

This draft document does not constitute a formal publication of ENISA and does not necessarily represent state-of the-art; this is a draft version of the candidate EU cybersecurity certification scheme and is solely distributed for consultation according to Article 49.3 of the Cybersecurity Act, and shall not be used for any other purpose. After consultation, ENISA may amend it.

Third-party sources are aimed to be quoted as appropriate, but due to the fact that this is a draft version, there may be a possibility that minor irregularities may be subject to correction. ENISA is not responsible for the content of the external sources including external websites referenced in this document. Flow charts, models, matrixes and statistics are also to be considered under draft status. No rights may be derived from them.

COPYRIGHT NOTICE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Following the request from the European Commission in accordance with Article 48.2 of the Cybersecurity Act[1] (hereinafter referred to as CSA as indicated in the glossary), ENISA has set up an Ad Hoc Working Group (AHWG) to support the preparation of a candidate EU cybersecurity certification scheme to serve as a successor to the existing schemes operating under the SOG-IS MRA (Senior Officials Group Information Systems Security Mutual Recognition Agreement).

Based on the outcomes from this AHWG, launched on November 27th, 2019 and composed of twenty (20) selected members representing industry (e.g., developers, evaluators), as well as around twelve (12) participants from accreditation bodies and EU Members States, regular discussions within the ECCG and after an internal review, ENISA has consolidated the following candidate scheme.

The EUCC scheme (Common Criteria based European candidate cybersecurity certification scheme) looks into the certification of ICT products cybersecurity, based on the Common Criteria, the Common Methodology for Information Technology Security Evaluation, and corresponding standards, respectively, ISO/IEC 15408 and ISO/IEC 18045.

The Common Criteria have proven particularly efficient in the last two decades in Europe for the certification of integrated circuits and smartcards and have therefore contributed to enhance the level of security of electronic signature devices, for means of identification such as passports, banking cards and tachographs for lorries.

Furthermore, they have been used intensively for the certification of the cybersecurity of ICT software products.

This scheme will improve the European Union Internal Market conditions for ICT products, and as a result also have positive effects for ICT services and ICT processes relying on such products.

The candidate EUCC scheme addresses the necessary requirements associated with the definition of a scheme, as defined under article 49.1 of the CSA, prescribing that the requirements of articles 51, 52 and 54 of the CSA shall be met.

It contains in addition background information associated to the requirements that provides clarification on the requirements and allows to illustrate a particular choice or to justify a particular case as expected by the CSA.

Finally, it addresses, based on the experience of the AHWG participants, some recommendations to the ECCG for the adoption and maintenance of the new scheme.

This version of the scheme has been updated based on the comments received through the public consultation and from the ECCG. Major changes relate to the:

- addition and clarification of definitions;
- systematic cooperation with the ECCG for the development of guidance documents supporting the scheme;
- clarification of activities related to the maintenance of certificates;
- clarification of deadlines associated to the handling of non-conformities, non-compliances and vulnerabilities;
- modification of the status of the new patch management process, now in annex and for trial use;
- modification of the logo associated to the certificates, allowing to establish an additional specific logo for the scheme and to mention the evaluation level achieved in addition to the CSA level;
- clarification of the peer assessment requirements and simplification of the associated annex;
- update of annexes 7 and 9 based on their recent evolution within the SOG-IS, and the addition of one annex related to ST sanitization.

[1] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCILof 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 (Cybersecurity Act).

GLOSSARY

For the purpose of this scheme, the following definitions apply, in addition and support of the definitions established under Article 2 of the CSA and the definitions included in the main document supporting this scheme, the Common Criteria for Information Technology Security Evaluation.

Term or concept	Abbreviation	Definition
Authorisation		Attestation by a NCCA that a CAB meets the specific or additional requirements related to its technical competence to evaluate defined in Article 54.1(f).
Assurance Family "Vulnerability Analysis"	AVA_VAN	Assurance family related to Vulnerability analysis defined by the CC Part 3. Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs. Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users. For this scheme, the AVA_VAN level determines the evaluation level as defined in Article 52.8.
Computer Emergency Response Team	CERT	Historic term for an expert group that handles computer security incidents.
Certificate maintenance		Process of analysing whether a set of one or more changes affects the assurance of the certified ICT product and then making a decision based on collected evidence.
Certification Body	CB	Third-party conformity assessment body operating certification schemes [ISO/IEC 17065]. NOTE1: The CB is in charge of the activities of certification related to the issuance of certificates; activities related to evaluation and testing are performed by the ITSEF (see associated definition). NOTE2: Under provisions of Art. 58(4), a NCCA can act as a CB. The term CB applies then to both a private CAB CB related body, and a NCCA acting as a CB. NOTE3: An issuer of certificates is considered an equivalent to a CB for this scheme.
Common Criteria	CC	Common Criteria for Information Technology Security Evaluation, composed of: Part 1: Introduction and general model Part 2: Security functional components Part 3: Security assurance components NOTE: the CC designate the Common Criteria for Information Technology Security Evaluation, under their applicable ISO/IEC 15408 version or under their applicable version published on https://www.commoncriteriaportal.org/cc/
Common Evaluation Methodology	CEM	Common Methodology for Information Technology Security Evaluation. NOTE: the CEM designates the Common Methodology for Information Technology Security Evaluation under its applicable ISO/IEC 18045 version or under its applicable version published on https://www.commoncriteriaportal.org/cc/.

Common Vulnerabilities and Exposures	CVE	List of entries, each containing an identification number, a description, and at least one public reference, for publicly known cybersecurity vulnerabilities.
Composite product evaluation/certification		Evaluation and certification procedures put in place to allow a product (e.g. smart card), as a combination of multiple parts (e.g. a hardware integrated circuit (IC) part and a software part composed of a platform and an application) often developed by different actors with specific objectives, to take directly into consideration the results of the assessment of one part (e.g. the IC certification) for the assessment of the other parts.
Conformity Assessment Body	CAB	Conformity assessment body as defined in point (13) of Article 2 of Regulation (EC) No 765/2008. NOTE: a CAB designates both the certification body (CB) and the internal or external testing laboratory (ITSEF). Where requirements are defined in this scheme for a CAB, they shall apply to both. If they only apply to the CB or the ITSEF, then the terms CB or ITSEF are used.
CyberSecurity Act	CSA	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 (Cybersecurity Act).
Evaluation		Combination of the selection and determination functions of conformity assessment activities [ISO/IEC 17065]. NOTE1: Evaluation tasks can include activities such as design and documentation review, sampling, testing, inspection and audit [ISO/IEC 17065]. NOTE2: In the context of the scheme, evaluation can be defined as assessment of an ICT product or a protection profile against the security evaluation criteria and security evaluation methods to determine whether or not the claims made are justified [CC Part 1]. NOTE3: Evaluation activities are performed by an ITSEF.
Evaluation Assurance Level	EAL	Well formed package of security assurance requirements [CC Part 3]. NOTE: EAL relate to assurance levels defined in the CSA as described in Section 4.
Evaluation Technical Report	ETR	Report established by an ITSEF serving as the principal basis for the Certification Report. NOTE: The objective of the ETR is to present all verdicts, their justifications and any findings derived from the work performed during the evaluation, including errors found during the development of the ICT product or Protection Profile and any exploitable vulnerabilities discovered during the evaluation. The ETR may contain protected information as necessary to justify evaluation results.
Impact Analysis Report	IAR	Document recording the analysis of the impact of changes to a certified ICT product.
Maintenance Report		Publicly available document that describes the results of a maintenance process applied to a certified ICT product. NOTE: A maintenance report motivates the decision related to the associated certificate.
Manufacturer or provider of the ICT certified product		The manufacturer or provider of an ICT product corresponds to the developer in the Common Criteria terminology when it comes to providing the evidence elements as required by the methodology (CC Part 3).
Market surveillance		Activities carried out and measures taken by public authorities to ensure that products comply with the requirements set out in therelevant Community harmonisation legislation and do not endanger health, safety or any other aspect of public interest protection (REGULATION (EC) No 765/2008).
National Cybersecurity Certification Authority	NCCA	A national cybersecurity certification authority is defined by Article 58.7 of the CSA.

		As such, unless explicitly mentionned, a NCCA is to be understood as the supervisory body, and not the CAB issuing certificates at level 'High' as provided by Article 56.6 of the CSA.
Non-compliance / Non-conformity		Non-compliance: not-fulfilment of a requirement related to provisions of the scheme or certificate. Non-conformity: not-fulfilment of a requirement related to technical standards or security objectives defined in Article 51 of the CSA.
Protection Profile	PP	Implementation independent set of security requirements for a category of ICT product that meets specific consumer needs.
Review		Verification of the suitability, adequacy and effectiveness of the evaluation, and the results of this activity, with regard to fulfilment of specified requirements by an object of conformity assessment [adopted from ISO/IEC 17000].
Scheme maintenance		Process of updating a certification scheme.
Security Assurance Requirement	SAR	Activities related to the assessment of the security of the ICT product to be certified. A catalogue of SAR is defined in the CC Part 3.
Security Functional Requirement	SFR	Security objectives of the ICT product to be certified. A catalogue of SFRs is defined in the CC Part 2.
Security Target	ST	Implementation-dependent statement of security needs for a specific identified TOE [CC Part 1].
Senior Officials Group Information Systems Security	SOG-IS	Committee with a long-term mandate to advise the Commission on action to be undertaken in the field of the security of information systems, installed by EU Council Decision of March 31st 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC) on common information technology security evaluation criteria.
SOG-IS Mutual Recognition Agreement	SOG-IS MRA	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates (applicable version 3.0, January 2010).
Subcontracting (of an evaluation task)		Assignment of an evaluation task of a CB to an external testing laboratory pursuant to Annex, point 9 of Regulation (EU) 2019/881.
Target of Evaluation	TOE	Set of software, firmware and/or hardware possibly accompanied by guidance [CC Part 1] that is subject to evaluation within the ICT product. The TOE may be a subset of the ICT product.
Technical Domain		Common technical framework defined for higher assurance levels of certification corresponding to AVA_VAN.4 and 5 and associated to a particular technology. Allows, among other, to define a common understanding of the attack potential and related attack methods for that technology. Its application relates also to the capabilities of CAB to perform such evaluations.
Testing Laboratory / Evaluation Facility	ITSEF	Third-party conformity assessment body that performs one or more of the following activities: - calibration - testing - sampling, associated with subsequent calibration or testing [adopted from ISO/IEC 17025]. NOTE1: In the context of the scheme, a testing laboratory carries out determination and selection functions as a part of conformity assessment evaluation activities. NOTE2: ITSEF (IT Security evaluation facility) is equivalent to Testing laboratory/Evaluation facility. It can be a) internal to a CAB, or b) an external entity to which the CAB acting as a CB subcontracts the evaluation. Where requirements are defined in the EUCC scheme for an ITSEF, they shall apply to both the internal and external entities. NOTE3: In the context of the EUCC scheme, the ITSEF is separated from the CB in terms of operations.

1. SUBJECT MATTER AND SCOPE

REFERENCE ARTICLE(S) OF THE CSA

Article 1.2 (S*ubject matter and scope): This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the State in areas of criminal law*.

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

a) the subject matter and scope of the certification scheme, including the type or categories of ICT products, ICT services and ICT processes covered.

The Common Criteria based European cybersecurity certification scheme (the EUCC scheme) covers the certification of ICT products.

The Common Criteria based European candidate cybersecurity certification scheme, hereinafter referred to as EUCC scheme) shall allow for the cybersecurity certification of ICT products according to ISO/IEC 15408 and the Common Criteria (CC), as defined in Chapter 3, EVALUATION STANDARDS.

The EUCC scheme may cover any type of ICT product addressing the European Union Internal Market, with the conditions that the ICT product shall:

- embed a meaningful set of security functional requirements as described by the CC Part 2;
- aim at reaching the assurance levels ‘substantial’ or ‘high’ of the CSA covered by this scheme.

The EUCC scheme shall cover the assessment of vulnerabilities of cryptographic implementations into the security functionalities of an ICT product in accordance with the requirements of the evaluation criteria and methodology defined in Chapter 3, EVALUATION STANDARDS.

Potential conditions regarding the achievable levels of certification shall apply, as described in Chapter 4, ASSURANCE LEVELS.

The EUCC shall in addition provide the possibility to cover additional elements as foreseen by Article 54 of the CSA, under the conditions defined by Chapter 24, ADDITIONAL ELEMENTS OF THE SCHEME:

- the certification of Protection Profiles[2];
- rules for the protection of information related to cybersecurity certification.

BACKGROUND INFORMATION

According to CC Part 1: *“The Common Criteria (CC) permits comparability between the results of independent security evaluations. The CC does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software.”*

Even when this scheme could theoretically address any ICT product, it is best suited for those that try to reach the ‘substantial’ and ‘high’ assurance levels of the CSA. Other schemes may be more appropriate to support the certification of ICT products that are less demanding in terms of levels of assurance.

Regarding cryptography, CC Part 1 indicates that: *“The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the CC. Should independent assessment of mathematical properties of cryptography be required, the evaluation scheme under which the CC is applied must make provision for such assessments.”*

[2] Protection profiles (PP) allow to define an implementation independent set of security requirements for categories of ICT products that meet specific consumer needs; PP are widely used by consumer groups and communities of interest, may become standards and be referenced into EU regulation.

The SOG-IS community has established with the SOGIS Agreed Cryptographic Mechanisms v1.1 document, a first building block for the analysis of the suitability of cryptographic mechanisms.

The need to extend the scope of the EUCC scheme with Protection Profile certification and security of information rules, was established by the AHWG based on current practices under the SOG-IS MRA and urgent needs. Associated conditions and more detailed background information are provided in Chapter 24, ADDITIONAL ELEMENTS OF THE SCHEME.

2. PURPOSE OF THE SCHEME

REFERENCE ARTICLE(S) OF THE CSA

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

b) a clear description of the purpose of the scheme and of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme.

The EUCC scheme may serve as a successor to the EU national schemes operating under the SOG-IS MRA, identified in Chapter 16, NATIONAL OR INTERNATIONAL SCHEMES.

It may allow to improve the Internal Market conditions, and to enhance the level of security of ICT products dedicated to security (e.g., firewalls, encryption devices, gateways, electronic signature devices, means of identification such as passports, …) as well as of any ICT product embedding a security functionality (i.e., routers, smartphones, banking cards, medical devices, tachographs for lorries, …).

By offering two (2) security assurance levels, 'substantial' and 'high', it shall cover a large variety of demanding security requirements, though not addressing the basic level that may be offered by schemes that are less demanding in terms of evaluation evidence and cover less stringent security requirements.

Users of the scheme may be:

- manufacturers or providers who wish to assess the security quality of their ICT products through third party certification;
- providers of ICT services or ICT processes who wish to benefit from the security evidence of certified ICT products for their clients;
- regulatory authorities who wish to establish security and assurance requirements on ICT products within their regulations and directives;
- end users who wish to comply with a regulation or gain security evidence on the ICT products that protect their sensitive assets.

To express their security requirements, both functional and in terms of assurance, these communities may use the methodology described in Chapter 24, ADDITIONAL ELEMENTS OF THE SCHEME to establish a Protection Profile for a category of products to be certified, or may establish an individual Security Target for individual products to be certified.

The EUCC scheme can serve the certification of many different types of generic and sector specific ICT products. As such, it is more of a horizontal scheme. Users of the scheme may establish Protection Profiles to express their security requirements.

In order to reduce the evaluation effort while keeping the necessary level of confidence, the EUCC scheme may allow for composite product certification[3]. Such certifications shall meet the conditions set out in Chapter 9, NECESSARY INFORMATION FOR CERTIFICATION.

When considering the cybersecurity certification of an ICT product, or the use of a certified ICT product, the different stakeholders including public bodies and the private sector shall consider the following characteristics of the EUCC scheme:

- a European harmonized quality of certificates for the ICT products aiming to reach the assurance levels 'substantial' and 'high' of the CSA, through independent third party assessment, national authorities involvement, and where necessary peer assessment;
- several sub-levels of assurance allowing to pursue a trade-off between assurance and the cost of evaluation and certification;
- a large catalogue of available and standardised security functionalities and assurance requirements offered by the CC and further described in Chapter 4, ASSURANCE LEVELS, that can be selected to define EU harmonised community security requirements through Protection Profiles in many security and sectorial fields;

[3] e.g. of an application on top of a certified platform, or of a platform on top of a certified IC.

- an ICT product life cycle with its guidance documentation included in the scope of the evaluation and a possible reuse of results between certifications, facilitating a lean schedule and cost structure;
- a large availability of supporting documents allowing for a good preparation of certification activities;
- a new set of harmonised activities of maintenance of certificates and of monitoring and handling of non-compliances and non-conformities;
- new harmonised conditions for vulnerability handling and a fast track assessment procedure for patches;
- new security conditions for the protection of information used for certification;
- a continuity with previous national certification schemes, both in terms of quality of the certificates, as in terms of compatibility of methodology, allowing for a smooth transition to the new scheme, both in terms of certificates and bodies implied into certification (CBs and ITSEFs), especially at the assurance level ‘high’;
- a new possibility offered for private actors to engage into cybersecurity certification activities for the ‘substantial’ assurance level, and to combine them with other sectorial certification activities;
- an EU-wide maintenance of the EUCC scheme, for continuous improvement.

BACKGROUND INFORMATION

CC Part 1 states that: *“[…] The evaluation results may help consumers to determine whether these IT products fulfil their security needs. The CC is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality. The CC is intentionally flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT products […] Whereas an ST always describes a specific TOE (e.g. the MinuteGap v18.5 Firewall), a PP is intended to describe a TOE type (e.g. firewalls). The same PP may therefore be used as a template for many different STs to be used in different evaluations. […] In general an ST describes requirements for a TOE and is written by the developer of that TOE, while a PP describes the general requirements for a TOE type, and is therefore typically written by:*

- *A user community seeking to come to a consensus on the requirements for a given TOE type;*
- *A developer of a TOE, or a group of developers of similar TOEs wishing to establish a minimum baseline for that type of TOE;*
- *A government or large corporation specifying its requirements as part of its acquisition process.”*

Regarding the advantages to consider for the selection of this scheme for the cybersecurity of ICT products, some are directly related to the characteristics of the scheme (e.g. reusability of certification activities, possibility to establish Protection Profiles).

In addition:

- Maintenance of certificates and monitoring compliance have been broadly developed for the EUCC scheme to give assurance that the security of the product is maintained.
- Common Criteria are harmonized criteria, recognized by international standardization committees of ISO and IEC that are continuously maintained by a wide international and European structured community, composed of technical and organizational representatives, working together for the sole purpose of enhancing the standard.
- The CC provide a (kind of pseudo-formal) language to represent security functions, mechanisms and actions to evaluate them. The CC are flexible, as they provide a catalogue of families and functions and operations to use and extend them, to describe any kind of ICT product, whether hardware, firmware or software, or their combination.
- The CC have the largest catalogue of peer reviewed and product independent security functional requirements (SFR) and security assurance requirements (SAR) making them applicable to a wide variety of ICT products.
- the CC have allowed a good catalogue of industry approved baseline requirements through Protection Profiles.
- In addition to the security of a product, the CC allow to check the development site security and the development process security.
- Certification under this scheme at ‘high’ assurance levels stems from the authorization of a Governmental agency.
- Many countries and users value certification against the CC: the CC have a long-standing history with respect to its recognition by fifteen (15) EU countries and more than thirty (30) countries in total, at their Federal and Government level. In addition, more than 4500 products have been already CC certified and used by billions of users all over the world.
- The CC enable consumers to have an impartial assessment of an ICT product: such an assessment is also a security evaluation, as the CC include an analysis and testing of the product for conformance to specific

security requirements. This increases the consumer's level of confidence in and reliance on the security of the certified ICT product.

- Flexible set of evaluation assurance levels: multiple levels of assurance are defined in the CC and have been mapped with two assurance levels of the CSA. This allows covering a large number of different markets security assurance needs as, the higher the level of assurance the product has, the more proof there is for its security with an increasing rigorous method of testing.
- The scheme includes specific measures to allow the prompt recognition of certified ICT products as it includes rules for the implementation and use of a dedicated labelling framework. Such framework has been designed to foster the placement of certified products both within and beyond the EU single market.

3. EVALUATION STANDARDS

REFERENCE ARTICLE(S) OF THE CSA

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

> *c) references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme.*

The EUCC scheme is based on the CC and the CEM, with an additional set of supporting elements, further defined in Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS.

Certified Protection Profiles may also be defined as applicable or reference standards for specific stakeholders' communities.

Evaluations shall be based on the following standards:

- Common Criteria for Information Technology Security Evaluation, under their applicable ISO/IEC 15408 version or under their applicable version published on https://www.commoncriteriaportal.org/cc/, and composed of:
  - CC Part 1: Introduction and general model;
  - CC Part 2: Security functional components;
  - CC Part 3: Security assurance components;
- and simply referred to as the Common Criteria or the CC into this candidate scheme;

- Common Methodology for Information Technology Security Evaluation, under its applicable ISO/IEC 18045 version or under its applicable version published on https://www.commoncriteriaportal.org/cc/, simply referred to as the CEM into this candidate scheme.

Certificates issued shall indicate which version/release of the CC and CEM have been used for the evaluation and certification.

Evaluation shall also take in consideration supporting elements established as to allow the harmonised interpretation of these standards. As further defined in Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS, such elements shall be either mandatory supporting elements integrated as annexes into this scheme, or guidance supporting documents developed in cooperation with the ECCG and provided by ENISA on its website dedicated to cybersecurity certification.

Where necessary, the different stakeholders of ICT products cybersecurity certification may define Protection Profiles as technical specifications. Such technical specifications may be adopted as standards by a national, EU or International standardization organization (Reg. UE 1025/2012[4]) and certified according to the requirements of this scheme. ENISA shall provide on its cybersecurity certification website a list of these Protection Profiles.

In addition, the following standards shall apply for the accreditation of the conformity assessment bodies that perform the evaluation and certification activities, in support of Article 60.1-2 and Annex.19-20 of the CSA:

- ISO/IEC 17065, for the conformity assessment body or national authority in charge of the activities of certification, hereinafter designated as certification body (CB);
- ISO/IEC 17025, for the part of a third-party conformity assessment body or national authority, or the subcontractor of a CAB or national authority, that is in charge of the activities of evaluation, hereinafter designated as testing laboratory (ITSEF).

[4] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation.

BACKGROUND INFORMATION

ISO/IEC 15408 and ISO/IEC 18045 have been since their creation an adoption of the Common Criteria (CC) and the Common Methodology for Information Technology Security Evaluation (CEM), which have been maintained as technical specifications by the Common Criteria community under the CCRA.

The ongoing revision of both standards at ISO will allow to introduce the advanced criteria offered by release 5 of the CC related to the introduction of the concepts of Base-PP, PP-Module and PP-Configuration. Therefore, when PP-Modules are introduced into the definition of an ICT product for its evaluation, the technical specifications shall currently apply in addition to the standards.

The Common Methodology for Information Technology Security Evaluation (CEM), states in its Introduction the following: "*The CEM recognises that not all questions concerning IT security evaluation will be answered herein and that further interpretations will be needed. Individual schemes will determine how to handle such interpretations, although these may be subject to mutual recognition agreements.*"

In order to harmonize evaluation and certification practices and to facilitate the mutual recognition of certificates, the SOG-IS community has therefore established a long series of supporting documents that refine the requirements from the two main standards. Most of these documents have not been submitted for standardisation, and are key for the new CC Scheme as well and therefore will be added, when for mandatory application, to the EUCC Scheme.

Certain EU communities of stakeholders, or EU regulatory authorities may decide to set up Protection Profiles that are developed within EU or international standardisation bodies, to be further referenced as applicable standards or technical specifications within a regulation. These PPs should be certified, as offered by the scheme in Chapter 24, ADDITIONAL ELEMENTS OF THE SCHEME, and then considered for their publication on the ENISA website dedicated to cybersecurity certification.

4. ASSURANCE LEVELS

REFERENCE ARTICLE(S) OF THE CSA

Article 52.6 *A European cybersecurity certificate that refers to assurance level 'substantial' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities. Where any such evaluation activities are not appropriate, substitute evaluation activities with equivalent effect shall be undertaken*.

The EUCC scheme covers assurance levels 'substantial' and 'high' of the CSA.

Article 52.7 *A European cybersecurity certificate that refers to assurance level 'high' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the risk of state-of- the-art cyberattacks carried out by actors with significant skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing. Where any such evaluation activities are not appropriate, substitute activities with equivalent effect shall be undertaken.*

Article 52.8 *A European cybersecurity certification scheme may specify several evaluation levels depending on the rigour and depth of the evaluation methodology used. Each of the evaluation levels shall correspond to one of the assurance levels and shall be defined by an appropriate combination of assurance components*.

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

d) where applicable, one or more assurance levels.

Certification under this scheme shall cover the assurance levels 'substantial' and 'high' of the CSA.

The assignment to the assurance levels of the CSA shall be based on the use of the assurance components for vulnerability assessment defined in CC Part 3 as follows:

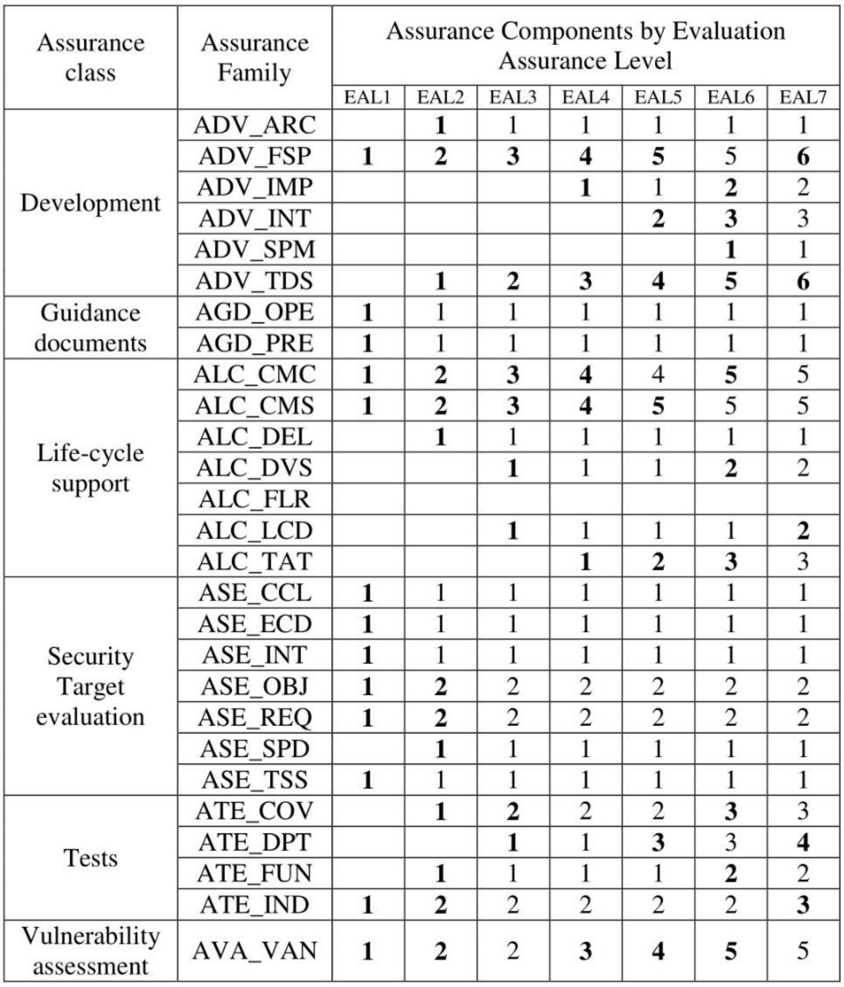
- AVA_VAN.1 and AVA_VAN.2 map to the assurance level 'substantial' of the CSA;
- AVA_VAN.3 to AVA_VAN.5 map to the assurance level 'high' of the CSA.

All dependencies, as defined in the CC Part 3, that apply to the selected AVA_VAN level shall be applied[5] and included into the applicable Security Assurance Requirements for the evaluation.

Preferably, all assurance components of the evaluation assurance level (EAL) defined by the CC Part 3 that is associated to the selected AVA_VAN level shall be applied, in accordance with the associated table.

[5] As an example from the CC Part 3, the direct dependencies that apply for AVA_VAN.3 Focused vulnerability analysis are:
ADV_ARC.1 Security architecture description
ADV_FSP.4 Complete functional specification
ADV_TDS.3 Basic modular design
ADV_IMP.1 Implementation representation of the TSF
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_DPT.1 Testing: basic design

Table 1: Evaluation assurance level summary (excerpt from CC Part 3)



Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
Guidance documents	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
Life-cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
Security Target evaluation	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**3**	3	**4**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

Where an AVA_VAN level is associated with multiple EALs, either EALs may be chosen.

The choice of a lower EAL level than the one(s) associated to the AVA_VAN level in the previous table may remain possible, under the conditions that:

- The chosen EAL shall not be more than two (2) levels lower than the lowest EAL associated to the AVA_VAN level;
- The resulting assurance level shall be treated as an augmentation of the chosen EAL as defined by the CC Part 3 and in accordance with Annex 1, ASSURANCE PACKAGE DECLARATION IN A CERTIFICATE.

The selected AVA_VAN level shall determine the corresponding CSA assurance level for the ICT product and the rules to apply for the certification of the concerned ICT product.

Therefore, as consequences for illustration on a few sample cases:

- when selecting AVA_VAN.2 that is according to the CC Part 3 in both evaluation assurance levels EAL2 and EAL3:
    - all dependencies of AVA_VAN.2 defined in the CC Part 3 are applied;
    - all assurance activities of EAL2 should at least be considered for the evaluation;
- a certificate related to the evaluation assurance level EAL3, that by definition embeds AVA_VAN.2, shall be considered as a certificate at the 'substantial' assurance level of the CSA;
- a certificate at EAL3 augmented with AVA_VAN.3 and associated dependencies is possible and shall be considered as a certificate at the 'high' assurance level of the CSA.

The possibility to evaluate and certify using the assurance components for vulnerability assessment AVA_VAN.1 and AVA_VAN.2 shall be based on the general provisions of this scheme.

The possibility to evaluate and certify using the assurance components for vulnerability assessment AVA_VAN.3 shall be based on the general provisions of this scheme with the addition of the requirements established for the CSA assurance level 'high' along this scheme.

The possibility to evaluate and certify using the assurance components for vulnerability assessment AVA_VAN.4 and AVA_VAN.5 shall be based on the general provisions of this scheme with the addition of the requirements established for:

- CSA assurance level 'high' along this scheme;
- Technical Domains as defined in Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS.

As a general rule, where no Technical Domain has been defined for a technology of ICT products, associated certificates shall not claim a vulnerability assessment level above the AVA_VAN.3 component.

Certification above AVA_VAN.3 for ICT products that are not covered by a Technical Domain shall only be possible based on a specific Protection Profile defined and certified under this scheme that includes guidance for the specific evaluation methodology, and is annexed to the scheme for this purpose. The guidance requirements for the PP may only be omitted if the risk owner (e.g. a representative of an operator, national policy maker, regulator) of the end application case described in the PP agrees.

ICT products certified according to these Protection Profiles shall be considered with high attention under the peer assessment mechanism encompassed in this scheme.

A certificate issued under this scheme shall indicate the CSA assurance level and the CC AVA_VAN and EAL levels satisfied by the evaluation of the ICT product, as well as the SAR components. It shall indicate any limitation related to the maximum levels that the CAB can achieve in accordance with this scheme.

ENISA may provide in cooperation with the ECCG guidance as how to select the proper assurance level based on risk assessment.

BACKGROUND INFORMATION

The CC have defined in their Part 3 the assurance family "Vulnerability Assessment', addressing the possibility of exploiting vulnerabilities introduced in the development or the operation of the TOE.

There are three main factors in performing a vulnerability analysis, namely:

1. the identification of potential vulnerabilities:
    a. Search of the public domain (CVE, CERT, etc.);
    b. Search of the evaluation evidence (within design documents, user guidance documents, etc.);
2. the assessment to determine whether the identified potential vulnerabilities could allow an attacker with the relevant attack potential to violate the SFRs:
    a. Flaw Hypothesis (analytical approach to find potential vulnerabilities, define priorities);
3. penetration testing to determine whether the identified potential vulnerabilities are exploitable in the operational environment of the TOE.

The following five different levels have been defined for that assurance class, and "*Levelling is based on an increasing rigour of vulnerability analysis by the evaluator and increased levels of attack potential required by an attacker to identify and exploit the potential vulnerabilities*."

- AVA_VAN.1 Vulnerability Survey
    - TOE resistance against BASIC Attack Potential (AP)
- AVA_VAN.2 (Unstructured) Vulnerability Analysis
    - TOE resistance against BASIC AP
- AVA_VAN.3 Focused (Unstructured) Vulnerability Analysis
    - TOE resistance against ENHANCED-BASIC AP
- AVA_VAN.4 Methodical Vulnerability Analysis
    - TOE resistance against MODERATE AP
- AVA_VAN.5 Advanced Methodical Vulnerability Analysis
    - TOE resistance against HIGH AP

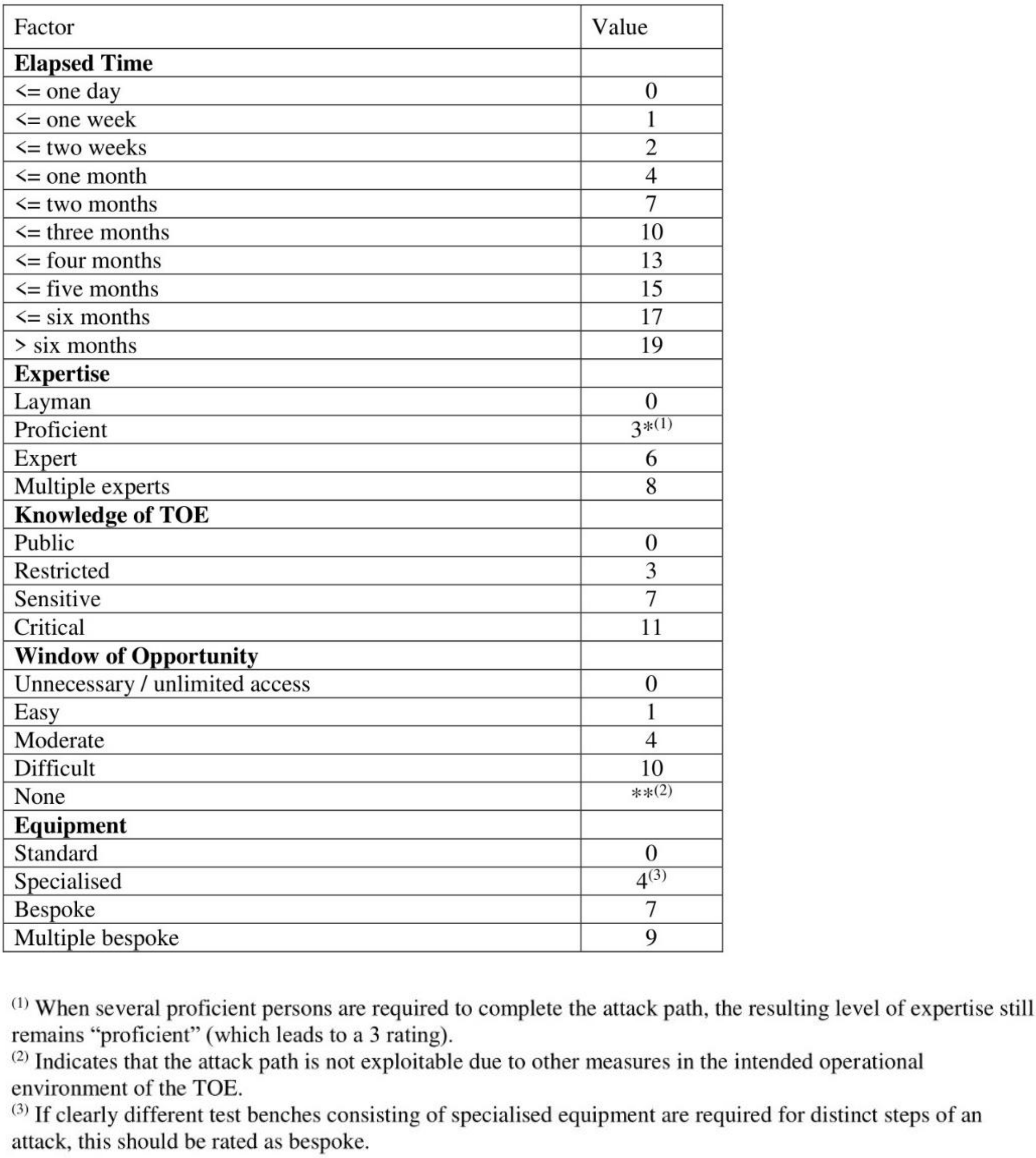
This class has therefore been selected as the most representative class to fulfil the requirements of Article 52.1 and its generic requirement in its section 1: "*The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident*."

Indeed, according to the CEM, “*The following factors should be considered during analysis of the attack potential required to exploit a vulnerability:*

a) Time taken to identify and exploit (Elapsed Time);
b) Specialist technical expertise required (Specialist Expertise);
c) Knowledge of the TOE design and operation (Knowledge of the TOE);
d) Window of opportunity;
e) IT hardware/software or other equipment required for exploitation.”

The CEM has defined a table for the calculation of the attack potential:

Table 2: Calculation of attack potential (excerpt from the CEM)

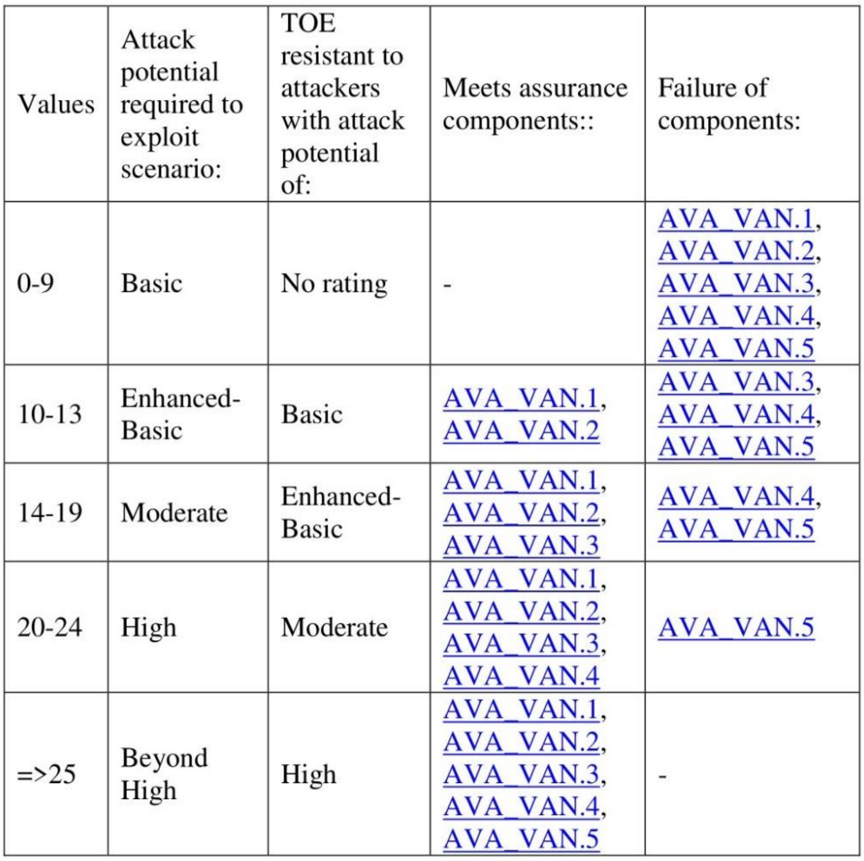


Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3*[1]
Expert	6
Multiple experts	8
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**[2]
Equipment	
Standard	0
Specialised	4[3]
Bespoke	7
Multiple bespoke	9

[1] When several proficient persons are required to complete the attack path, the resulting level of expertise still remains “proficient” (which leads to a 3 rating).
[2] Indicates that the attack path is not exploitable due to other measures in the intended operational environment of the TOE.
[3] If clearly different test benches consisting of specialised equipment are required for distinct steps of an attack, this should be rated as bespoke.

Based on these elements for the calculation of the attack potential, the CEM defines the rating of the resistance of a product with the following table:

Table 3: Rating of vulnerabilities and TOE resistance (excerpt from the CEM)



Values	Attack potential required to exploit scenario:	TOE resistant to attackers with attack potential of:	Meets assurance components::	Failure of components:
0-9	Basic	No rating	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10-13	Enhanced-Basic	Basic	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
14-19	Moderate	Enhanced-Basic	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
20-24	High	Moderate	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>25	Beyond High	High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

In addition, the CC introduce the concept of dependencies between assurance components, meaning that when selecting one assurance component, one shall, in order to fulfil the requirements of the standard, apply as well related components. These dependencies have been as well required for the mapping with the CSA assurance levels.

What the standard defines for the first level of the Vulnerability Assessment class, AVA_VAN.1, is the following: "*A vulnerability survey of information available in the public domain is performed by the evaluator to ascertain potential vulnerabilities that may be easily found by an attacker. The evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. Penetration testing is performed by the evaluator assuming an attack potential of Basic*."

The term *Basic attack potential* used in the CC is misleading when comparing to the assurance level basic of the CSA, as:

- it requires the need to collect at least 10 points to reach that level considering the previous table;
- the type of activities undertaken for assessing conformance to AVA_VAN.1 already meets the following requirement of the CSA for the 'substantial' level as defined under Article 52.6:
  - A "review to demonstrate the absence of publicly known vulnerabilities".

In order to fulfil the additional requirements of Article 52.6 for this 'substantial' assurance level:

- a "verification of the compliance of the security functionalities of the ICT product, ICT service or ICT process with its technical documentation"(Recital 89) or "testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities" (Article 52.6 of the CSA);

the necessity to consider the full package of assurance components associated to the EAL level directly including the AVA_VAN level has been established.

Indeed, EAL1 that embeds AVA_VAN.1 also requires functional independent testing of the ICT product through its component ATE_IND.1.

However, this general rule to consider all dependencies or a full EAL package may be subject to derogation, as foreseen by the CC Part 3, 6.1.3.4: "*In specific situations the indicated dependencies might not be applicable. The PP/ST author, by providing rationale for why a given dependency is not applicable, may elect **not** to satisfy that dependency*."

AVA_VAN.2 being based on the same attack potential as AVA_VAN.1, it is considered of the same CSA 'substantial' assurance level.

AVA_VAN.3 allows to address the next category of attack potential, defined as Enhanced-Basic in the CC, and adds the following activity for the evaluator: "*The evaluator shall perform an independent, focused vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE*."

Based on the 14-19 points range to address that Enhanced-Basic level, this level is addressing the need to resist to attackers:

- with significant skills and resources: an expertise level of proficient on bespoke equipment, or of expert on specialised equipment, which would "attribute" ten (10) points in either case;
- attacking for a rather lengthy period (over one (1) month), which would attribute seven (7) points.

This is therefore considered to satisfy the requirements of Article 52.7 for the CSA assurance level 'high'.

Based on the definition above, this is at the same time dictating the evaluator with at least the same levels of skills and equipment described above to perform a focused vulnerability analysis using sensitive product information that the 'real' attacker should not get access to. This is clearly beyond the requirement associated to the 'substantial' level to provide '*a review to demonstrate the absence of publicly known vulnerabilities*'.

Regarding the even higher levels of AVA_VAN (4 and 5), the necessity to define a common framework that would allow to harmonise the judgement of experts has been introduced by the SOG-IS community, in order to take into consideration the evaluation context introduced in the CC Part 3, chapter 5.5:

"*In order to achieve greater comparability between evaluation results, evaluations should be performed within the framework of an authoritative evaluation scheme that sets the standards, monitors the quality of the evaluations and administers the regulations to which the testing laboratories and evaluators must conform. The CC do not state requirements for the regulatory framework. However, consistency between the regulatory frameworks of different evaluation authorities will be necessary to achieve the goal of mutual recognition of the results of such evaluations. A second way of achieving greater comparability between evaluation results is using a common methodology to achieve these results. For the CC, this methodology is given in the CEM. Use of a common evaluation methodology contributes to the repeatability and objectivity of the results but is not by itself sufficient. Many of the evaluation criteria require the application of expert judgement and background knowledge for which consistency is more difficult to achieve. In order to enhance the consistency of the evaluation findings, the final evaluation results may be submitted to a certification process. The certification process is the independent inspection of the results of the evaluation leading to the production of the final certificate or approval, which is normally publicly available. The certification process is a means of gaining greater consistency in the application of IT security criteria. The evaluation schemes and certification processes are the responsibility of the evaluation authorities that run such schemes and processes and are outside the scope of the CC.*"

Such common framework has been defined through the development of Technical Domains that allow, among other, to define a common understanding of the attack potential and related attack methods for higher levels of certification (including AVA_VAN.4 and 5) and for particular types of ICT products. Its application also relates to the possibility of a CAB to perform such evaluations, further defined in Chapter 6, SPECIFIC REQUIREMENTS APPLICABLE TO A CAB.

Where no specific Technical Domain has been defined for an ICT product to be certified above AVA_VAN.3, or in the absence of the appropriate authorisation for the CAB to certify for the concerned specific Technical Domain of the ICT product to be certified, the certificate emitted under this scheme should be limited to the AVA_VAN.3 level.

The possibility to derogate to this general rule that certification above AVA_VAN.3 necessitates a Technical Domain has been introduced, and this should only occur through the definition and certification of a Protection Profile that becomes integral part of the mandatory requirements for this scheme and constitutes integral part of an Annex to the scheme. The strong incitation for inclusion of associated certified products into the scope of the peer assessment will allow to mutually check the methodology, tools and skills used for the evaluation of these products, and to be in an even better position to further define Technical Domains derived from these specific PPs.

5. CONFORMITY SELF-ASSESSMENT

REFERENCE ARTICLE(S) OF THE CSA

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

e) an indication of whether conformity self-assessment is permitted under the scheme.

The EUCC Scheme shall not allow for conformity self-assessments.

The scheme does not permit conformity self-assessments.

BACKGROUND INFORMATION

The scheme does not cover the CSA assurance level basic, which is the only level that allows for conformity self-assessments in accordance with Article 53.1 of the CSA.

Moreover, §8.2.3 of the CEM requires separation of roles (e.g., sponsor, evaluator, evaluation authority), as a way to prevent undue influence from improperly affecting an evaluation.

6. SPECIFIC REQUIREMENTS APPLICABLE TO A CAB

REFERENCE ARTICLE(S) OF THE CSA

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

f) *where applicable, specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements.*

Annex, REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES:
19. *Conformity assessment bodies shall meet the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of conformity assessment bodies performing certification of ICT products, ICT services or ICT processes.*

20. *Conformity assessment bodies shall ensure that testing laboratories used for conformity assessment purposes meet the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of laboratories performing testing.*

CAB, including their testing laboratories, are subject to specific requirements in addition to their accreditation for the ‘high’ assurance level of certification.

In accordance with Annex.19 of the CSA, a certification body (CB) shall be accredited with the relevant standard, ISO/IEC 17065. It shall in addition be authorised by its NCCA to produce certificates at the assurance level ‘high’ of the CSA.

A testing laboratory (ITSEF) including its staff performing evaluations for a certification body, be it the internal testing laboratory of a conformity assessment body or an external testing laboratory in the case where testing is performed by a subcontractor, shall be technically competent for the related tasks.

For the assurance level ‘substantial’, this technical competence shall be assessed through the accreditation of the testing laboratory according to ISO/IEC 17025 for evaluations according to ISO/IEC 18045 in conjunction with ISO/IEC 15408.

ENISA may provide, with the support of the European co-operation for Accreditation, and in cooperation with the ECCG, guidance for harmonised interpretation of ISO/IEC 17025 for the EUCC scheme taking into account related standards such as ISO/IEC 19896-3.

For the assurance level ‘high’, in addition to the accreditation of the testing laboratory according to ISO/IEC 17025, the EUCC scheme provides for the following specific requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements:

- specific requirements shall concern technical competences related to specific testing activities and shall apply only as regards certificates issued at assurance level ‘high’;
- requirements shall apply both to internal testing laboratories of conformity assessment bodies and to the external ones in cases where testing is performed by a subcontractor.

These ITSEFs and their concerned personnel shall be required to meet the following requirements:

(a) to have the necessary expertise and experience in performing the specific testing activities to determine the product’s resistance against specific attacks (penetration testing) assuming an attack potential of ‘basic-enhanced’ as described in the CC (AVA_VAN.3 Focused Vulnerability Analysis).

(b) For the technical domains defined in Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS:

- to have the necessary expertise and experience in performing the specific testing activities necessary to methodically determine the resistance of the product against attacks exercised in the product’s operational environment assuming the corresponding attack potential of either ‘moderate’ or ‘high’ as described in the CC (AVA_VAN.4 Methodical vulnerability analysis, AVA_VAN.5 Advanced methodical vulnerability analysis);

- to be able to demonstrate the specific following technical competences:
  - for the ‘Smart Cards and similar devices’ Technical Domain, required capabilities from Annex 8;
  - for the ‘Hardware Devices with Security Boxes’ Technical Domain, required capabilities from Annex 10.

BACKGROUND INFORMATION

Requirements applicable to the CBs associated to their capability to issue certificates are only summarised here, as they are already defined under the general terms of the CSA.

The SOG-IS MRA and the CCRA both request as a basis the accreditation according to ISO/IEC 17025 of the ITSEFs that perform the evaluations. That is deemed sufficient for the ‘substantial’ level that is associated to AVA_VAN.1 and 2, according to the description of the evaluation level mapping of Chapter 4, ASSURANCE LEVELS.

Mutually approved interpretation of the accreditation standards for certification and testing laboratories activities could however be needed, and should then be defined as guidance for the scheme (with the support of European co-operation for Accreditation). ENISA can propose in cooperation with the ECCG related refinements, reusing the experience of various SOG-IS MRA members that developed such interpretations, and the use of the following potentially relevant standards:

- ISO/IEC 19896, Competence requirements for information security testers and evaluators, especially:
  - Part 1: Introduction, concepts and general requirements
  - Part 3: Knowledge, skills and effectiveness requirements for CC evaluators
- ISO/IEC 2nd WD 23532-1, Requirements for the competence of IT security testing and evaluation laboratories, especially:
  - Part 1: Evaluation for the CC

NOTE: ISO/IEC 19896-3 provides competency requirements for CC evaluators that can be used as a support in the evaluation process. However, it only addresses basic methodology competences and does not address the way to assess technology-specific knowledge and skills such as those required to perform ADV, ATE or AVA_VAN evaluation on a given product type, nor sector-specific knowledge that is typically required to perform ASE, APE or ACE evaluation. Additionally, specific skills required by CC evaluations may require additional competence assessment methods. For example, to assess skills related to formal methods.

For the assessment of the capabilities of an ITSEF to perform evaluations at the AVA_VAN.3 level, no detailed harmonised framework has been set up so far, although certification bodies proceed in general to this assessment considering:

- the experience of the ITSEF and associated personnel;
- their capabilities to determine the product’s resistance against specific attacks (penetration testing) assuming an attack potential of ‘basic-enhanced’ as described in the CC (AVA_VAN.3 Focused vulnerability analysis);
- the necessary interviews and/or tests of the evaluators, and the possible close monitoring by the CB of pilot evaluations at the considered level.

As a consequence, the harmonisation of the way to perform this assessment for this first version of the EUCC scheme is to be achieved through the peer review and peer assessment mechanisms and ENISA may further develop in cooperation with the ECCG guidance based on these peer reviews/assessments.

For each technical domain, the SOG-IS MRA has set up specific requirements to which an ITSEF shall comply to be declared capable to perform such evaluations:

- Minimum ITSEF Requirements for Security Evaluations of Smart cards and similar devices, in Annex 8;
- Minimum ITSEF Requirements for Security Evaluations of Hardware Devices with Security Boxes, in Annex 10,

Examples within Annex 8 of which requirements are embedded for the IC evaluators in terms of skills and knowledge in the following technical areas are the:

- understanding of secure IC-based design (such as a smartcard, secure element, etc.) and production process in general of the IC design and manufacturing process;
- understanding of secure IC technology, its underlying principles and the development equipment used by secure IC manufacturers;
- understanding of secure IC-based ecosystem, with a strong knowledge of the related threats and attack techniques.

- knowledge and experience in hardware physical attack techniques that could compromise a secure IC and an ability to use the related equipment to stress the hardware layers. This includes the understanding of the IC underlying physical principles;
- knowledge and experience in physical disruptions that could change the secure IC behaviour, with the aim to subsequently downgrade the security of the IC-based device. The ability to use related equipment to conduct physical disruptions and the understanding of related physical effects on the hardware;
- knowledge and experience in cryptographic attack techniques and the ability to perform the analysis (including data-capture and signal processing procedures).

Additionally, for the other Technical Domain defined for the EUCC scheme, following required capabilities for composite evaluations refer to the logical architecture-related skills and knowledge of evaluators about:

- source code review, interface specifications (both native and protocols), content and resource management;
- supply chain integration aspects in the application environment;
- cryptographic software, both with or without dedicated hardware usage;
- virtual machines;
- software-related attacks.

7. NOTIFICATION AND AUTHORISATION OF CABS, FUNCTIONING OF CABS AND SUBCONTRACTORS

REFERENCE ARTICLE(S) OF THE CSA

Article 2.18: *'conformity assessment body' means a conformity assessment body as defined in point (13) of Article 2 of Regulation (EC) No 765/2008*.

Article 54.1.(f): *where applicable, specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements.*

Article 56.6.: *Where a European cybersecurity certification scheme adopted pursuant to Article 49 requires an assurance level 'high', the European cybersecurity certificate under that scheme is to be issued only by a national cybersecurity certification authority or, in the following cases, by a conformity assessment body:*

(a) upon prior approval by the national cybersecurity certification authority for each individual European cybersecurity certificate issued by a conformity assessment body; or

(b) on the basis of a general delegation of the task of issuing such European cybersecurity certificates to a conformity assessment body by the national cybersecurity certification authority.

Article 60.2.: *Where a European cybersecurity certificate is issued by a national cybersecurity certification authority pursuant to point (a) of Article 56(5) and Article 56(6), the certification body of the national cybersecurity certification authority shall be accredited as a conformity assessment body pursuant to paragraph 1 of this Article*.

Article 60.3.: *Where European cybersecurity certification schemes set out specific or additional requirements pursuant to point (f) of Article 54(1), only conformity assessment bodies that meet those requirements shall be authorised by the national cybersecurity certification authority to carry out tasks under such schemes.*

Regulation 765/2008.13.: *'conformity assessment body' shall mean a body that performs conformity assessment activities including calibration, testing, certification and inspection.*

Under this scheme, both certification bodies (CBs) and testing laboratories (ITSEFs) shall be assessed for authorisations to perform certification and evaluation at the assurance level 'high' of the CSA.

Notification

For each CAB issuing certificates (designated as a certification body or CB, according to the Glossary) notified in accordance with Article 61 of the CSA, the notification shall include:

- the specified CSA assurance level ('substantial', or 'high');
- where the CSA assurance level is 'high', the AVA_VAN level up to which the CB can issue certificates, and where applicable, the technical domains for which certification is offered;
- where applicable, the list of the ITSEFs performing evaluations for the CB, including the AVA_VAN level up to which each ITSEF can evaluate, and where applicable, the technical domains for which evaluation is offered.

Authorisation

A NCCA shall, for the authorisation of a CAB to carry out tasks under the EUCC scheme, proceed to the assessment of the approval performed by the CAB in compliance with the specific requirements described in Chapter 6 SPECIFIC REQUIREMENTS APPLICABLE TO A CAB of the internal testing laboratory of this CAB and, in cases where testing is performed by a subcontractor, of the external testing laboratory.

This assessment may include, for each ITSEF:

- conducting structured interviews to determine that the ITSEF and its personnel have the necessary expertise and experience in the relevant activities;
- reviewing evidences of two pilot evaluations performed by the ITSEF as part of the approval procedure of the CAB and evaluating their performance.

In cases where testing is performed by a subcontractor, authorised certification bodies shall provide the necessary technical support to their NCCA for the assessment of the ITSEFs, and shall participate to their audit on a regular basis (two (2) years minimum).

This support shall also cover the assessment that the ITSEFs meet the stringent security requirements necessary for the protection of sensitive or protected information relating to ICT products or protection profiles under evaluation and to the process of evaluation itself, as requested by Chapter 24, ADDITIONAL ELEMENTS OF THE SCHEME.

Unless duly justified, authorised CBs and associated ITSEFs shall participate and provide technical support to the maintenance of the scheme.

When establishing a request for certification under this scheme at the assurance level ‘high’ of the CSA, a manufacturer or provider may consult any ITSEF associated to an authorised CAB for availability and estimation of resources and costs for the evaluation, and may contract directly to one or more of these ITSEFs. However, the following determinations apply:

- it shall only establish a contract with an ITSEF that has been properly notified with the CB at the relevant level;
- the ITSEF shall inform the CB of the resources (man-days) allocated for the evaluation;
- the CB remains the main responsible body for the resulting certificate.

Subcontracting and the use of 3rd party facilities

Subcontracting shall be allowed according to requirements stipulated in accreditation standards, relevant to the CB and ITSEF activities i.e. ISO/IEC 17065 and ISO/IEC 17025, respectively.

An ITSEF deemed competent for a Technical Domain may only subcontract its work within the Technical Domain under the following conditions:

- activities shall only be taken in charge by an ITSEF competent for the considered Technical Domain;
- further subcontracting shall only be possible with the consent of the CB, the NCCAand the manufacturer or provider of the ICT product;
- the activities shall be performed under the full control and responsibility of the subcontracting ITSEF;
- only partial subcontracting of AVA_VAN activities shall be allowed.

Further subcontracting shall not affect the confidentiality, objectivity or impartiality of the evaluation activities, in accordance with the requirements of paragraphs 7, 9 and 16 of the Annex to the CSA. The above mentioned consent of the CB shall require the delivery by the ITSEF and its subcontractor of the necessary content to assess that the subcontractor is able to fulfil all necessary requirements.

When an ITSEF uses other facilities (e.g., third parties independent of both the ITSEF and the company(ies) developing and producing the TOE), appropriate security measures shall be applied to protect the vendor's information and samples and the know-how of the ITSEF. This may require additional measures should the TOE need to remain in the third party facility unattended. This may also require careful consideration for obtaining repeatability of test results if the sample has been removed from site or the equipment settings modified prior to completing the TOE analysis.

The use of the third party facility shall be outlined in the evaluation plan and approved by the manufacturer or provider and by the CB, while the ITSEF remains responsible for the work done.

When the ITSEF uses bespoke equipment at the third party facility, the evaluator shall be present and instruct the operating personnel. To instruct the operating personnel, evaluators shall have sufficient knowledge of the TOE, the equipment, and the purpose of the test.

BACKGROUND INFORMATION

A certification scheme relies on multiple activities including certification and evaluation activities. As a CB may outsource broadly its evaluation activities, especially at the assurance level ‘high’, the notification shall allow to indicate the level that each individual member can achieve, and authorisation take full consideration of the underlying capabilities of the ITSEFs.

This will allow the necessary competition and therefore applicants to consult and select the subcontractor(s) of their choice, provided conditions defined in this section.

For the assessment of the ITSEFs, the technical skills of the CBs should be involved and benefit to their NCCA.

8. SPECIFIC EVALUATION CRITERIA AND METHODS

REFERENCE ARTICLE(S) OF THE CSA

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

> *g) the specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the security objectives referred to in Article 51 are achieved.*

The selection of appropriate functional (SFR) and assurance (SAR) requirements from the CC may allow to cover a large variety of security objectives of Article 51 of the CSA. In addition, Supporting Documents providing harmonised interpretation of the standards are introduced.

In addition to some specific provisions of this scheme, the CC strongly contribute to meet the security objectives defined by Article 51 of the CSA. This shall occur through the selection of relevant components within the following classes/families of the catalogue of Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs):

Table 4: Candidate SFR and/or SAR to fulfil Security objectives defined by Article 51

Security objectives defined by Article 51	Candidate class/families of SFR and/or SAR from the CC
(a) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process;	-SFR Class FCO: Communication -SFR Class FCS: Cryptographic support, including SFR Family FCS_COP: Cryptographic operation -SFR Class FDP: User data protection, including SFR Family FDP_UCT: Inter-TSF user data confidentiality transfer protection
(b) to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process;	-SFR Class FDP: User data protection, including SFR Family FDP_SDI: Stored Data Integrity and SFR Family FDP_UIT: Inter-TSF user data integrity transfer protection -SFR Family FCS_COP: Cryptographic operation
(c) that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;	-SFR Class FDP: User data protection, including SFR Family FDP_SDI: Stored Data Integrity and SFR Family FDP_UIT: Inter-TSF user data integrity transfer protection -SFR Family FCS_COP: Cryptographic operation -SFR Family FMT_MSA Management of security attributes -SFR Family FMT_SMF Specification of Management Functions
(d) to identify and document known dependencies and vulnerabilities;	-SFR Class FDP: User data protection -SAR Family ALC_FLR: Flaw remediation -SAR Family ALC_CMS: CM Scope -SAR Class ASE: Security Target
(e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;	-SFR Class FAU: Security audit, including SFR Family FAU_GEN: Security audit data generation -SFR Class FTA: TOE access
(f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;	-SFR Class FAU: Security audit, including SFR Family FAU_SAR: Security audit data review -SFR Family FMT_MSA Management of security attributes -SFR Family FMT_SMF Specification of Management Functions

(g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;	-SAR Class AVA: Vulnerability assessment, including SAR Family AVA_VAN: Vulnerability analysis
(h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;	-SFR Class FPT: Protection of the TSF, including SFR Family FPT_RCV: Trusted recovery
(i) that ICT products, ICT services and ICT processes are secure by default and by design;	-SAR Family ALC_TAT: Tools and techniques -SAR Family ADV_ARC: Security Architecture -SAR Family ADV_TDS: TOE Design -SAR Family ASE_SPD: Security problem definition
(j) that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.	-SAR Class AVA: Vulnerability assessment -SAR Family ALC_FLR: Flaw remediation

In accordance with the CC, extended components to the existing catalogue of SFRs and SARs may be defined in order to better suit to the above objectives in a particular ICT product, when necessary.

A user of certified products or an applicant to certification shall decide against which security objectives he/she decides to evaluate the ICT product(s) and select the applicable requirements, either in a Protection Profile or a Security Target of the individual ICT product. ENISA may provide in cooperation with the ECCG associated guidance for this selection, based on risk assessment methods or tools.

However, by default, any evaluation shall be based on the use of the SAR Class AVA: Vulnerability assessment and the SAR Family ALC_FLR: Flaw remediation, as to ensure that ICT products are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.

As indicated in Chapter 3, EVALUATION STANDARDS, the two (2) applicable standards for evaluation, ISO/IEC 15408 and ISO/IEC 18405, shall be supported by mandatory supporting elements and guidance supporting documents:

- Mandatory supporting elements are described in the Annexes of this document and are for mandatory application (their application scope may however be limited). They contain a consistent set of interpretations that specify the use of the criteria and methodology within a particular field or domain of technology and shall be used where relevant. The Evaluation Technical Report and the Certification Report shall identify which mandatory supporting elements have been used;
- Guidance supporting documents contain non-binding advice and recommendations their use is non-mandatory, although recommended. The objective of guidance documents is for developers, evaluators and issuers of certificates to improve the evaluation and certification process. Guidance documents may contain background material to support the understanding of the evaluation approach or any other information and entail no obligations for any of the involved actors. However, where relevant to the ICT products to be certified, the possibility to reference and to use them for evaluation shall always be considered.

Mandatory supporting elements may be for trial use, for a certain period: where applicable, such a status shall be indicated, as well as the applicable period of trial use.
The objective of the trial use period shall be to gain experience in the application of the requirements of the elements in the context of a product evaluation. The application of the elements for trial use shall be mandatory for the certification of concerned ICT products, but during the trial phase period it may occur on a case-by-case basis that additional support from the authority or body in charge of the certification is required to interpret the trial use elements, would problems with their applications arise.
When necessary interpretations have been identified during the trial use phase, they shall be shared among the ECCG dedicated structure that will support the maintenance of the scheme in order to improve the elements in a next version of the related documentation, and the ECCG shall establish which elements ENISA may provide on its website before any formal revision of the documentation has been adopted.

All guidance documents supporting this scheme shall be established in cooperation with the ECCG and shall be published on the ENISA website dedicated to cybersecurity certification.

Following elements shall be applied as mandatory supporting elements for use during evaluations of ICT products regardless of the type of the ICT products or their assurance level:

- Annex 1, containing conditions for Assurance package declaration in a certificate.

The two (2) following Technical Domains shall allow for the certification of technology related ICT products to the assurance levels AVA_VAN.4 and AVA_VAN.5, provided the application of specific additional methods, techniques and tools for their evaluation. These Technical Domains are:

- Smart Cards and Similar Devices - where significant portions of the required security functionality depend upon hardware features at a integrated circuit level (e.g., smart card hardware/ICs, smart card composite products, TPM[6] used in Trusted Computing, digital tachograph cards, etc.)
- Hardware Devices with Security Boxes - where significant portions of the required security functionality depend upon a hardware physical envelope with counter-measures (a so-called "Security Box") against direct physical attacks (e.g., payment terminals, tachograph vehicle units, smart meters, taxi meters, access control terminals, Hardware Security Modules, etc.).
  Note: In cases where the physical protection (“security box”) requirements defined in a Protection Profile developed by a standards body recognised by the EU differ from those generally applying in the domain (whether greater or smaller), the PP requirements and associated methodology shall take precedence.

Following elements shall be applied as mandatory supporting elements for evaluations of ICT products related to these Technical Domains:

- for both Technical Domains, Annex 2, containing Minimum Site Security Requirements;
- for the Technical Domain Smart carts and similar devices, additional evaluation methods, techniques and tools included in:
  - Annex 3, containing conditions related to the Application of CC to Integrated Circuits;
  - Annex 4, containing Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices;
  - Annex 5, containing conditions related to the Certification of "open" smart card products;
  - Annex 6, containing conditions related to Composite product evaluation for Smart Cards and similar devices;
  - Annex 7, containing conditions related to the Application of Attack Potential to Smartcards;
  - Annex 8, containing Minimum ITSEF requirements for Security Evaluations of Smart cards and similar devices;
- for the Technical Domain Hardware Devices with Security Boxes, additional evaluation methods, techniques and tools included in:
  - Annex 9, containing conditions related to the Application of Attack Potential to HW Devices with Security Boxes;
  - Annex 10, containing Minimum ITSEF requirements for Security Evaluations of Hardware Devices with Security Boxes.

Other chapters of this document may request the application of additional mandatory supporting elements as to support requirements associated to the EUCC scheme. These elements shall also be provided in annexes to this scheme.

Where the ICT product undergoes a composite product evaluation, sensitive information shall be shared between the ITSEF that proceeded to the evaluation which results are reused and the ITSEF that proceeds to the evaluation of the composed product. This information sharing shall be done through a structured documentation, the evaluation technical report (ETR) for composition. ENISA shall provide a template for the ETR for composition[7].

BACKGROUND INFORMATION

The mapping between the security objectives defined by Article 51 of the CSA and the selected SFR or SAR classes can be further checked through the review of the CC. ENISA may provide in cooperation with the ECCG a supporting guidance document to this mapping.

To support the necessary development and evolution of mandatory supporting elements, the concept of trial use has been introduced. It allows to verify for a certain period of time the validity of the requirements they establish, with the

[6] Trusted Platform Modules.

[7] https://www.sogis.eu/documents/cc/domains/sc/JIL-ETR-template-for-composition-v1-1.pdf is the current applicable template for the SOG-IS MRA related composite evaluations, which may serve as a technical basis for the EUCC scheme ETR for composition template.

possibility to derogate and still certify and then to inform the community of the necessary modifications, before the supporting elements become fully applicable.

Technical domains have been established based on the following characteristics:

- in the technologies covered by the scope of Smart Cards and Similar Devices, an attacker will often be able to obtain physical access to the device (or a set of devices); the device may well contain critical information such as security credentials/keys and part of the security functionality required of the device will relate to self protection either by active (tamper detection) or passive means (such as tamper resistant coatings). This contrasts with standard multipurpose hardware as used in general processing equipment (such as a PC).

The evaluation approach needs to consider all hardware specific aspects of vulnerability analysis including those that require significant additional equipment and resources. Such devices are frequently composed from elements produced by different developers (e.g., hardware, smart card operating system, and application) and may involve production across a range of development sites (e.g. IC design, mask production, fabrication, characterisation, etc). These factors must also be consistently taken into account during evaluation and certification.

- in the technologies covered by the scope for Hardware Devices with Security Boxes, an attacker will often be able to obtain physical access to the device (or a set of devices). The device may contain critical information such as security credentials/keys, or could be used also for secure entry of credentials/keys and a significant part of the security functionality required of the device will relate to self protection against physical attacks. These self protection counter-measures or the “security box” of such devices is composed of physical protection counter-measures based on hardware and software active mechanisms. Usually these mechanisms involve also passive protections as an inherent part of the provided security functionality (e.g., metallic shields or armoured plating, wire meshing, chemical protections like epoxy resin, etc.) in conjunction with sensors and electronic anti-tampering mechanisms (like secure data erasing, alarm generation or component emergency destruction).

The evaluation approach needs to consider all software, firmware and hardware specific aspects of vulnerability analysis including those that may require significant additional equipment and resources. Such devices are also frequently composed from discrete parts produced by different developers. These factors must also be consistently taken into account during evaluation and certification.

9. NECESSARY INFORMATION FOR CERTIFICATION

REFERENCE ARTICLE(S) OF THE CSA

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

> *h) where applicable, the information which is necessary for certification and which is to be supplied or otherwise be made available to the conformity assessment bodies by an applicant.*

Article 55 *Supplementary cybersecurity information for certified ICT products, ICT services and ICT processes*

The necessary information for certification shall include relevant evidence for evaluation. It may include previous evaluation results.

Each applicant shall provide to the conformity assessment body the necessary information for the cybersecurity evaluation.

This shall include all relevant evidence as required under *Developer action elements,* and within the appropriate format as requested by *Content and presentation elements,* by the CC Part 3 for the selected assurance level and associated Security Assurance Requirements. The evidence shall include, where necessary, detailed information on the ICT product and its source code.

As part of a new certification, it shall be possible to reuse evaluation results from another ICT product certification. The applicant may therefore provide to the CAB previous evaluation results including those related to the lifecycle of the product or the applicant's patch management approach to be re-used as evidence. The CAB shall reuse such results for its tasks when the provided evidence conforms to the requirements of such evidence required by the CAB and the authenticity of the evidence can be confirmed.

Where the CAB approves the ICT product to undergo a composite product certification, all necessary elements as defined in Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS shall be made available to the CAB performing the composite evaluation, in accordance, where applicable, with the Mandatory Supporting elements established for a Technical Domain.

Necessary information shall be supplied to the CAB, unless the CAB agrees to get access to that information in a different way[8].

In addition, for this scheme, each applicant shall provide to the conformity assessment body, in accordance with the rules defined in Chapter 23, SUPPLEMENTARY CYBERSECURITY INFORMATION - ARTICLE 55 a link to the supplementary cybersecurity information as defined by Article 55 of the CSA. This shall allow the CAB to integrate the link into the cybersecurity certificate as requested by Chapter 17, CONTENT AND FORMAT OF CERTIFICATES.

The EUCC scheme may request that part or all of such supplementary information shall or may be subject to an assessment by the CAB; this shall be indicated in the relevant Chapter(s).

General rules regarding the protection of the information provided by an applicant shall comply with the requirements established under Chapter 24, ADDITIONAL ELEMENTS OF THE SCHEME.

BACKGROUND INFORMATION

Information that is required by the applicant based on the same underlying standard (the CC) will facilitate migrations from the SOG-IS MRA to the new scheme, and where feasible, reuse, under the conditions defined for the scheme. Such a reuse might relate to the life cycle of the ICT product (such as the sites where the product is developed or produced), or procedures (such as patch management), that are applicable to several products and have already been assessed within previous evaluations and certifications.

[8] The CAB may for example agree to get access to the information on the premises of the manufacturer or provider.

In addition to the presentation to the CAB of the link to the supplementary cybersecurity information as required by Article 55 of the CSA, that will be inserted into the certificate (see Chapter 17, CONTENT AND FORMAT OF CERTIFICATES), the need to make part of the content of that information available to the CAB has been provisioned. It will permit to check, where necessary, that this information is valid, complete, accurate and up-to-date in accordance with the requirements of the relevant chapters, such as rules on vulnerability handling.

Rules related to the security of information have been established in order to allow for a harmonised protection of sensitive and proprietary information of developers undergoing certification.

10. MARKS AND LABELS

REFERENCE ARTICLE(S) OF THE CSA

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

i) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used.

The European Cybersecurity Certification Framework may provide for a label and associated mark.

When available, such a label shall be specifically implemented for this scheme, in order to allow its application on each certificate, certified ICT product and related documentation.

A label and associated mark shall only be used when the certificate is awarded and until its expiration: the non-respect of this condition shall be considered as an irregularity, as defined by Chapter 11, RULES FOR MONITORING COMPLIANCE.

Without prejudice to the rules for monitoring compliance as described under Chapter 11, RULES FOR MONITORING COMPLIANCE, depending on the circumstances, the nature and impact of the non-respect, wrong use, misuse, abuse of the mark and or label may have other legal implications in the field of IP right protection, possible criminal allegations (e.g. fraud, deceit), market surveillance regulations related to consumer protection (e.g. misleading and or unlawful comparative advertising or distribution of products). These legal implications are outside the scope of this EUCC scheme.

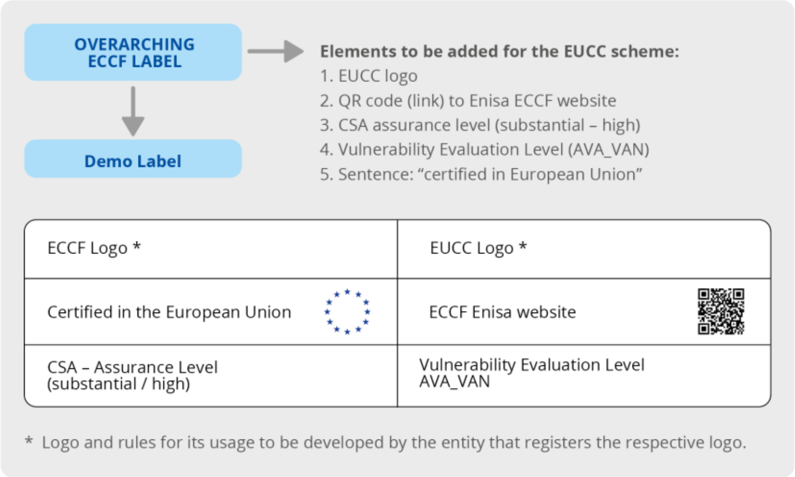
It is foreseen that a label is associated with the European Cybersecurity Certification Framework, and specifically implemented for each scheme, including the EUCC scheme.

BACKGROUND INFORMATION

A label and associated mark, established for the European Cybersecurity Certification Framework and specifically implemented for this scheme, will allow to:

- highlight that the ICT product has been certified in the European Union and to provide immediate information regarding the certificate by making reference to the framework (ECCF), the evaluation scheme and the assurance level;
- make the certification easily recognizable as both the label and the associated mark may be printed on the package of the product, on technical documents and on leaflets used for marketing purposes;
- provide a direct link (in the form of a QR code) to the ENISA website (as per Article 50) - where all the information regarding the certificate are disclosed, including the current status of the certificate.

Figure 1: Demo label fo the EUCC scheme



Elements to be added for the EUCC scheme:

1. EUCC logo
2. QR code (link) to Enisa ECCF website
3. CSA assurance level (substantial – high)
4. Vulnerability Evaluation Level (AVA_VAN)
5. Sentence: "certified in European Union"

ECCF Logo *	EUCC Logo *
Certified in the European Union	ECCF Enisa website
CSA – Assurance Level (substantial / high)	Vulnerability Evaluation Level AVA_VAN

* Logo and rules for its usage to be developed by the entity that registers the respective logo.

The “demo label”, shows the basic information that the label associated with the scheme may contain:

- logo of the ECCF (to be registered, regulated and protected by the entity in charge of the enforcement of the labelling framework);
- logo of the EUCC (to be registered, regulated and protected by the entity in charge of the enforcement of the labelling framework);
- QR code pointing to the web portal of ENISA - as per the Article 50 of the CSA – and to the page where the effective status of the certificate of the product and the information regarding its lifecycle can be retrieved;
- CSA assurance level (with the introduction of a specific colour identifying each level) and related vulnerability evaluation AVA_VAN level;
- the sentence “Certified in the European Union”, together with the flag of the EU.

The introduction of the QR code will imply, as defined by Chapter 20, DISCLOSURE POLICY FOR CERTIFICATES, a procedure for the release of the QR code.

11. RULES FOR MONITORING COMPLIANCE

REFERENCE ARTICLE(S) OF THE CSA

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

j) rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements.

Monitoring rules are based on potential cases of non-compliances and non-conformity and shall consist of prevention, and detection measures.

Article 58 7. *National cybersecurity certification authorities shall:*

a) supervise and enforce rules included in European cybersecurity certification schemes pursuant to point (j) of Article 54(1) for the monitoring of the compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates that have been issued in their respective territories, in cooperation with other relevant market surveillance authorities;
b) monitor compliance with and enforce the obligations of the manufacturers or providers of ICT products, ICT services or ICT processes that are established in their respective territories and that carry out conformity self-assessment, and shall, in particular, monitor compliance with and enforce the obligations of such manufacturers or providers set out in Article 53(2) and (3) and in the corresponding European cybersecurity certification scheme;
c) without prejudice to Article 60(3), actively assist and support the national accreditation bodies in the monitoring and supervision of the activities of conformity assessment bodies, for the purposes of this Regulation;
d) monitor and supervise the activities of the public bodies referred to in Article 56(5);
f) handle complaints by natural or legal persons in relation to European cybersecurity certificates issued by national cybersecurity certification authorities or to European cybersecurity certificates issued by conformity assessment bodies in accordance with Article 56(6) or in relation to EU statements of conformity issued under Article 53, and shall investigate the subject matter of such complaints to the extent appropriate, and shall inform the complainant of the progress and the outcome of the investigation within a reasonable period;
g) provide an annual summary report on the activities conducted under points (b), (c) and (d) of this paragraph or under paragraph 8 to ENISA and the ECCG;
h) cooperate with other national cybersecurity certification authorities or other public authorities, including by sharing information on the possible non-compliance of ICT products, ICT services and ICT processes with the requirements of this Regulation or with the requirements of specific European cybersecurity certification schemes.

Article 58 8. *Each national cybersecurity certification authority shall have at least the following powers:*

a) to request conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statements of conformity to provide any information it requires for the performance of its tasks;
b) to carry out investigations, in the form of audits, of conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statements of conformity, for the purpose of verifying their compliance with this Title;
c) to take appropriate measures, in accordance with national law, to ensure that conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statements of conformity comply with this Regulation or with a European cybersecurity certification scheme;
d) to obtain access to the premises of any conformity assessment bodies or holders of European cybersecurity certificates, for the purpose of carrying out investigations in accordance with Union or Member State procedural law;
e) to withdraw, in accordance with national law, European cybersecurity certificates issued by the national cybersecurity certification authorities or European cybersecurity certificates issued by conformity

assessment bodies in accordance with Article 56(6), where such certificates do not comply with this Regulation or with a European cybersecurity certification scheme;

f) to impose penalties in accordance with national law, as provided for in Article 65, and to require the immediate cessation of infringements of the obligations set out in this Regulation.

Without prejudice to NCCA activities defined under Articles 58.7 and 58.8 of the CSA, monitoring compliance of ICT products with the requirements of the European cybersecurity certificates shall demonstrate their continued compliance with the specified cybersecurity requirements.

In particular, this monitoring shall allow where possible to avoid and where needed to detect the following general cases of non-compliance:

- a non-compliance in the application by a manufacturer or provider of the rules and obligations related to a certificate issued on their ICT product;
- a non-compliance in the conditions under which the certification takes place and that are not related to the individual ICT product;
- a non-conformity of a certified ICT product with its security requirements, which includes and is not limited to a:
    - change in the threat environment after the issuance of the certificate, which has an adverse impact on the security of the certified ICT product[9];
    - vulnerability identified and related to the certified ICT product, that has an adverse impact on the security of the certified ICT product.

The general monitoring of the certified ICT products shall be based on sampling, using generic criteria such as product type, evaluation level, manufacturer or provider, CAB and any relevant information brought to the knowledge of the NCCA (e.g. complaints, security events). The NCCAs on their respective territories and in cooperation with other relevant market surveillance authorities, shall sample annually a minimum of 5% of the products and at least one product per annum which received certificates in the previous year.

The NCCA shall involve in the monitoring the CB and where necessary the ITSEF of the certified ICT product. The monitoring shall consist in the re-assessment of the ICT product, as defined by Annex11, together - when necessary – with an audit to confirm or disprove the above-mentioned relevant information (e.g. complaints, security events) brought to the knowledge of the NCCA.

Where a product is selected the manufacturer or developer shall be informed of the selection reasons.

Re-assessments and audits if required shall be financially supported by the manufacturer or provider.

In addition to this general monitoring, the activities described hereinafter shall be undertaken.

The following deviations and irregularities shall be considered as potential non-compliances in the application by a manufacturer or provider of the rules and obligations related to a certificate issued on their ICT product:

- any deviation from the requirements applicable to the information supplied or made available to a CB or ITSEF, and that might be discovered after the emission of a certificate, such as:
    - a version of the information delivered that does not correspond to the ICT certified product;
    - self-established evidence that was not in-line with the reality of the product;
- any deviation from the requirements regarding the certificate content and the supplementary information as required by Chapter 9, NECESSARY INFORMATION FOR CERTIFICATION, Chapter 17, CONTENT AND FORMAT OF CERTIFICATES, Chapter 18, AVAILABILITY OF INFORMATION and Chapter 23, SUPPLEMENTARY CYBERSECURITY INFORMATION - ARTICLE 55, including and not limited to:
    - deviation from referencing the proper ICT product identifiers;
    - misalignment of the description of the description of the TOE scope[10];
    - deviation from constraints of the certificate including those of Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES[11];
    - deviations from the conditions of use of the scheme's marks and labels as defined in Chapter 10, MARKS AND LABELS;

[9] Not to be confused with the operational environment, for which the users take the sole responsability.

[10] e.g. suggesting the certificate covers the whole product rather than the actual TOE, by using a same or similar name for the TOE and the whole product .

[11] e.g. advertising a certified product after the product certificate has expired.

    - undue modifications or alterations of the certificate document as defined in Chapter 17, CONTENT AND FORMAT OF CERTIFICATES;
    - omission to provide or undue alteration of product specification and supplementary information as defined by Chapter 18, AVAILABILITY OF INFORMATION and Chapter 23, SUPPLEMENTARY CYBERSECURITY INFORMATION - ARTICLE 55;
- any deviation from the requirements on the certificate holder's obligations towards maintaining the certificate validity, such as:
    - failure to apply mandatory maintenance activities;
    - failure to implement and enforce mandatory processes as requested by the Terms and Conditions of a certificate and of the label;
    - failure to notify modifications to the development cycle and environment where applicable[12];
    - deviations from the certified product scope, including obligations from Article 56.8 of the CSA, including:undeclared modifications of the ICT product, its delivery processes, the development environment[13], the CMC list of TOE components[14], or employed tools[15].

Such non-compliance in the application by a manufacturer or provider of the requirements related to a certificate issued on their ICT product shall be monitored by:

1) requiring any applicant to a certificate to commit to the CB to a number of obligations, including but not limited to:
    - to transmit information to the CB and the ITSEF deemed reliable and that would not risk falsifying their judgment;
    - not to declare an object as certified while the evaluation is still undergoing;
    - to declare an object as certified only for the scope specified in the certificate;
    - to stop immediately the use of any advertisement mentioning the certification in the event of suspension or withdrawal of the certification;
    - to make sure that products manufactured in series and sold in link with the issued certificate are strictly identical to the one which was the object of certification;
    - to commit to scrupulously respecting the rules of use of the label established for the scheme;
2) using the following available dispositive to track the non-respect of the previous obligations :
    a. the activities of market surveillance established under Article 58.7.(a) of the CSA, with a report to the CB who issued the certificate;
    b. the quality measures in place within the CB, and the possibility to establish and handle complaints;
3) an assessment of the gravity of the irregularity by the CB with where necessary, the support of the ITSEF;
4) using the possibility of the dialog between the CB and the manufacturer or provider to try and solve minor issues, and of the provisions of Chapter 13, RULES RELATED TO NON-COMPLIANCE where necessary.

The NCCA shall be informed of the results of these activities.

In addition to the activities of market surveillance, NCCA may establish rules for a periodic dialog between the issuers of certificates and the certificates owners, as to formally check and report the respect of previously stated obligations.

ENISA may, for harmonisation into the EUCC scheme, provide in cooperation with the ECCG guidance on the commitments that may be part of an application request, with an indication of the associated gravity.

The following deviations shall be considered as potential issues related to non-compliance in the conditions under which the certification takes place and that are not related to the individual ICT product:

- failure to meet obligations regarding handling complaints towards maintaining the certificate validity, including:
    - obligations for auditing the scheme compliance of the CB, the ITSEF and the certificate holders related to certificate use as implicitly required by Article 58.8.(b) of the CSA;
    - obligations for supervising and enforcing CB's, ITSEF's and certificate holder's scheme compliance as implicitly required by Art. 58.7.(a) of the CSA;
    - obligations for complaint handling as implicitly required by Art. 58.7.(f);
- deviations from evaluation requirements:
    - unjustified deviation from the evaluation methodology and applicable supporting documents described under Chapter 3, EVALUATION STANDARDS;

[12] e.g. change of foundry for chips.
[13] e.g. upgrading a CMC.
[14] e.g. switch to different components when listed ones are discontinued.
[15] e.g. modifying ALC_TAT related tools.

  - deviations from expected evaluation competence, as described under Chapter 6, SPECIFIC REQUIREMENTS APPLICABLE TO A CAB.

Such non-compliance in the conditions under which the certification takes place and that are not related to an individual ICT product shall:

1) be avoided where possible through:
   a. the audits permitted through Article 58.8.(b) and (c);
   b. the permanent monitoring of the ITSEF by their Accreditation bodies and CB, as requested by Chapters 6 and 23;
2) be detected through:
   a. the quality process of the CB and the ITSEF, including the report to the NCCA of the identified issue, and the requirement associated to their accreditation to handle complains.

The following shall be considered as potential issues of non-conformity of a certified ICT product with its security requirements:

- a change in the threat environment which has an adverse impact on the security of the certified ICT product;
- a vulnerability identified and related to the certified ICT product, that has an adverse impact on the security of the certified ICT product.

Such non-conformity of a certified ICT product with its security requirements shall be monitored under the following responsibilities:

1) manufacturers and providers of ICT products shall:
   - monitor any vulnerability that would be relevant to their ICT product, either published by or received from end users and security researchers as defined in Article 55.1.(c), or discovered by the manufacturer/provider and inform the CB who issued the certificate about changes related to the statements of the respective certificate;
   - monitor the known dependencies and vulnerabilities identified by any other source that may apply to the certified product, and submit an impact analysis where necessary to their CB;
   - work in cooperation with the CB and where necessary with the NCCA to support their monitoring activities;
   - such activities may be assessed within the certification process of the ICT product, through the corresponding CC Part 3 assurance family ALC_FLR;
2) certification bodies and ITSEF shall;
   - monitor any vulnerability from any source that would be relevant to their scope of evaluation and certification;
   - report to their NCCA any detected vulnerability affecting the conformity of a certified ICT product to the requirements related to the certification.

Where deemed necessary by the CB or at the discretion of the NCCA, a series of evaluation tasks may be requested to be performed with the support[16] of the manufacturer or provider of the certified ICT product as to confirm the impact of a non-conformity.

These activities related to monitoring compliance shall be part of the annual summary report of a NCCA.

BACKGROUND INFORMATION

The requirements have been established considering:

- potential irregularities (as of Article 56.8 of the CSA): An irregularity affecting product compliance arises from the security claim as stated in the certificate and/or its underlying specification (objectives, assumptions, functionalities, etc.), the developer environment (ALC), product delivery (ALC_DEL), product testing (ATE), vulnerability assessment (AVA), and/or if chosen flaw remediation (ALC_FLR). Though such irregularities are addressed as a product's non-compliance post-certification, they may arise any time;
- potential gaps into the technical competencies of a CAB;
- potential vulnerabilities and modifications of a product or of its environment.

Associated non-compliance issues have been identified and counter-measures for the prevention and detection thereof established.

- [16] Where necessary, support shall imply financial support to described activities.

This process benefits of the provisions of the CSA:

- market surveillance installed by Article 58.7.(a);
- obligation on auditing the scheme compliance of CABs and certificate holders mandated by Article 58.8.(b);
- the right to contest certificates (Article 63.1), and the need to the responsible bodies or authorities to handle complaints regarding the validity of a certificate issued at assurance level ‘high’ (Article 58.7.(f), and therefore product compliance as required by Article 54.1.(j);
- a NCCA may – through the power of Article 58.8.(b) – investigate a complaint towards product compliance by auditing the certificate holder and issuer and thus pre-empt litigation. This legal construct in turn leaves certificates at assurance level ‘substantial’ without any precautionary measure for handling the complaint outside of court;
- such complaints therefore need to be handled at the level of the CAB and its NAB. Since Art 54.1.(j) demands rules for product compliance and no such legal requirement for complaint handling at assurance level ‘substantial’ exist, an obligation for the pursuit of such complaints was included. As a result, complaint handling was levelled to all assurance levels of the scheme;
- the necessity to address Vulnerability Handling into the scheme and to adopt new patching procedures.

As for the manufacturers or providers task to monitor the known dependencies and vulnerabilities: the Terms and Conditions of the certificate require that a manufacturer or provider monitors the threat landscape and notifies the CAB about any vulnerability in their certified product. An ITSEF may propose manufacturers or providers such a service.

Where necessary, the conditions to support new evaluation activities have been indicated, as they might have a financial impact.

12. CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES

REFERENCE ARTICLE(S) OF THE CSA

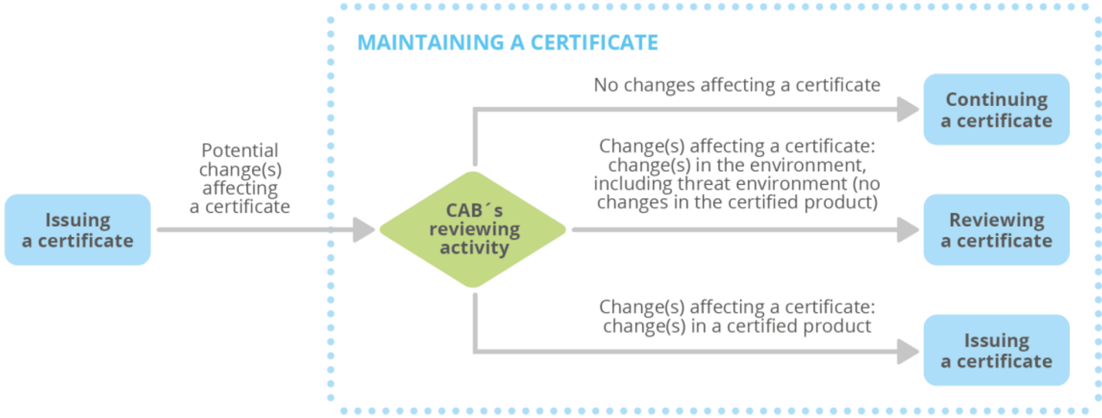
Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

k) where applicable, the conditions for issuing, maintaining, continuing and renewing the European cybersecurity certificates, as well as the conditions for extending or reducing the scope of certification.

Conditions for issuing, continuing and renewing certificates take into consideration multiple aspects such as expiration, non-conformity or non-compliance. They introduce the possibility of a fast track approach through patch management.

Introduction to processes related to the issuance and maintenance of a certificate
Several processes are related to the issuance and maintenance a certificate: a high-level overview is presented in the following picture:

Figure 2: High-level overview of processes related to the issuance and maintenance of a certificate


MAINTAINING A CERTIFICATE
Issuing a certificate
Potential change(s) affecting a certificate
CAB´s reviewing activity
No changes affecting a certificate
Continuing a certificate
Change(s) affecting a certificate: change(s) in the environment, including threat environment (no changes in the certified product)
Reviewing a certificate
Change(s) affecting a certificate: change(s) in a certified product
Issuing a certificate

The reference standard for these activities is ISO/IEC 17065 and in particular, its Clause 7.10, where ‘changes affecting a certificate’ are discussed[17].

Changes affecting the certificate can be of various nature and may be related to its technical content that could result in non-conformities, or related to other factors, including non-compliances[18]. Note that Annex 11, ASSURANCE CONTINUITY covers only part of the maintenance activities related to the certificate: it considers changes of technical nature which directly relate to the assurance attested by the certificate.

Conditions for issuing a certificate
A certification body (CB) shall only issue a certificate when the:

- applicant has committed to all obligations that need to be fulfilled under this scheme to obtain the certificate;
- evaluation of the ICT product is in line with the evaluation requirements set in this scheme for the requested selection of assurance components, and is successful;
- review by the CB of the evaluation results is successful and in line with the requirements of ISO/IEC 17065.

- [17] Note that the standard does not use the term ‘maintenance’.
- [18] see discussion on non conformities/non compliances in Chapter 11, RULES FOR MONITORING COMPLIANCE.

The CB shall monitor all evaluation reports provided by the ITSEF (including the Evaluation Technical Reports) to ensure that the conclusions are consistent with the evidence adduced and that the accepted evaluation criteria and evaluation methods have been correctly applied.

The certificate shall be related to the version of the ICT product evaluated, including its guidance documentation.

The CB shall establish a period of validity for the certificate that shall not exceed the maximum period defined in Chapter 19, PERIOD OF VALIDITY OF CERTIFICATES.

Conditions for maintaining, continuing and renewing a certificate

During the validity period of its certificate, the certified ICT product may remain stable and benefit from an unchanged threat environnement; in that case, the certificate will continue till its expiration date. This shall be confirmed by the CAB as part of its monitoring activities as described in Chapter 11, RULES FOR MONITORING COMPLIANCE.

In all other cases, the certified ICT product shall be subject to maintenance activities in response to changes affecting its certification. The maintenance activities shall encompass review and decision performed by the CB, and, where such activity is deemed necessary, evaluation performed by the ITSEF.

The maintenance activities may be initiated on the request of the owner of the certificate upon the following conditions:

- a soon to come expiration of the validity period of the certificate;
- a change of the certified ICT product, including a change in its lifecycle, which is not expected to and could have an impact on its security functionality;
- a request to refresh the vulnerability assessment, in order to prove that the resistance claims associated with the certificate still hold compared to state of the art attacks.

It shall be initiated upon the following conditions:

- when the ICT product has been selected through the sampling rule installed for the general monitoring of certified ICT products, as defined by Chapter 11, RULES FOR MONITORING COMPLIANCE;
- following a potential or actual non-conformity with security requirements, which includes and is not limited to:
  - a change in the threat environment which could have an adverse impact on the security of the certified ICT product;
  - a potential vulnerability identified and related to the certified ICT product, that could have an adverse impact on the security of the certified ICT product;
- following an identified non-compliance with the accreditation requirements of the CAB, the CSA provisions, or the scheme requirements, that affects the certification.

Depending on the nature of the previous conditions, and in accordance with the requirements established in Chapter 11, RULES FOR MONITORING COMPLIANCE, Chapter 13, RULES RELATED TO NON-COMPLIANCE and Chapter 14, RULES RELATED TO HANDLING VULNERABILITIES, the maintenance activities shall be triggered at the discretion of the manufacturer or provider of the ICT product, the CB, or the NCCA. The National Accreditation Body may also trigger maintenance activities where a complaint has been issued.

When the maintenance activities are initiated by the manufacturer or provider of the ICT product, the request to the CB shall be accompanied with an Impact Analysis report (IAR), in accordance with Annex 11, ASSURANCE CONTINUITY.

When the maintenance activities are initiated by any other party (CB, NCCA, and any stakeholder acting as a sponsor of the associated maintenance activities), the request shall be supported by a maintenance rationale containing a description of the potential or actual non-conformity or the identified non-compliance stated and its potential impact on the certificate.

Based on the IAR or the maintenance rationale, the CB shall validate whether some evaluation tasks are deemed necessary before its review and decision, and validate accordingly, with the support of the ITSEF the scope of and the workload associated to these tasks. The CB shall also validate the result of the necessary evaluation tasks once completed by the ITSEF.

The manufacturer or provider of the ICT product shall support[19] the ITSEF for the evaluation tasks deemed necessary, unless otherwise specified in Chapter 13, RULES RELATED TO NON-COMPLIANCE.

[19] Where necessary, support shall imply financial support to described activities.

A request for maintenance activities may identify a high level of urgency for changes/patches to the certified ICT product: where applicable, the CB may decide to authorise the application of the patch management process as defined by Chapter 14, RULES RELATED TO HANDLING VULNERABILITIES.

Where a patch management has been put in place according to the requirements of Annex 15, PATCH MANAGEMENT which is for trial use[20], the CB may also decide to authorise its application as a fast track approach to handle maintenance activities associated to functional changes to a product.

Upon review and decision of the CB, the maintenance activities shall result in one or the combination of the following decisions:

- continuing the certificate, corresponding to keeping the existing certificate alive, without change,
- renewing the certificate with a new validity period, corresponding to re-issuing the same certificate with a new validity period
- issuing a certificate with either an extended scope, a reduced assurance level, or a reduced scope of the certificate to still meet the current assurance level, potentially with a new validity period;
- suspending the certificate pending remedial action by the manufacturer or provider of the ICT product,
- withdrawing the certificate.

Decisions shall be accompanied with a Maintenance Report issued by the CB, in accordance with Annex 11, ASSURANCE CONTINUITY, and uniquely linked to the certificate; it shall motivate the decision and, where applicable, indicate any necessary change to the initial certificate.

In the case no maintenance has been requested for a certificate that has reached its expiration date, the certificate shall be subject to archiving. Archiving shall consist of still providing access to the certificate and associated information, with the clear indication that its expiration date has passed.

In the case a maintenance shall be initiated and no action was taken by any of the responsible parties in due time, the certificate shall be withdrawn.

The following table shall be considered by the CB to support the appropriate decision on most frequent possible cases.

Table 5: Nominal decisions associated with the maintenance of certificates

Cases	Nominal decisions
The same ICT product still meets its security requirements for certification.	Continue the certificate until its expiration date
The expiration date of the certificate has been reached and no request for maintenance has been submitted.	Archive the certificate
New evaluation tasks (refer to re-assessment defined in Annex 11) including vulnerability testing were performed on the same version of the ICT product and are successful.	Renew the certificate with potentially an extended validity period
The modified/patched version of the ICT product meets its security requirements for certification according to the developer's processes and no new evaluation tasks have been deemed necessary.	Issue a new certificate with a scope corresponding to the new version with the same validity period
New evaluation tasks (refer to re-evaluation defined in Annex 11) including vulnerability testing were performed on a modified/patched version of the ICT product and are successful.	Issue a new certificate with an extended scope corresponding to the modified version and with an extended validity period
Necessary evaluation tasks (refer to re-assessment defined in Annex 11) were performed and identify the same version of ICT product does not meet all applicable requirements, and a reduction of scope of the certificate would allow to maintain the security level.	Issue a new certificate with a reduced scope with possibly an extended validity period

[20] As defined in Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS.

Necessary evaluation tasks (refer to re-assessment defined in Annex 11) were performed and identify the same version of ICT product does not meet all applicable requirements, and a reduction of the assurance level would allow to maintain a certificate.	Issue a new certificate with a reduced assurance level with possibly an extended validity period
Necessary evaluation tasks (refer to re-assessment defined in Annex 11) were performed and identify the same version of ICT product does not meet all applicable requirements, and action is possible to maintain the certificate at the same level and with the same scope, though not immediately, or improper use of the certificate or of the mark is not immediately solved by suitable retractions and appropriate corrective actions by the manufacturer or provider.	Suspend the certificate pending remedial action by the manufacturer or provider of the ICT product
Necessary evaluation tasks were not performed.	Withdraw the certificate
Necessary evaluation tasks (refer to re-assessment defined in Annex 11) were performed and identify the same version of ICT product does not meet all applicable requirements.	Withdraw the certificate
Necessary maintenance activities were not performed in due time.	Withdraw the certificate

A certificate shall only remain in the ‘suspended’ status for a maximum duration of 3 months that may only be extended when the delay is due to a lack of availability of the CB, the ITSEF or the NCCA. In case no action is taken by the vendor in due time the status of certificate shall be changed into ‘withdrawn’ by the CB.

Any change of the status of a certificate shall be disclosed without undue delay according to the requirements of Chapter 20, DISCLOSURE POLICY FOR CERTIFICATES.

BACKGROUND INFORMATION

Requirements have been established considering the requirements associated with ISO/IEC 17065, and ISO/IEC 17067, Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes.

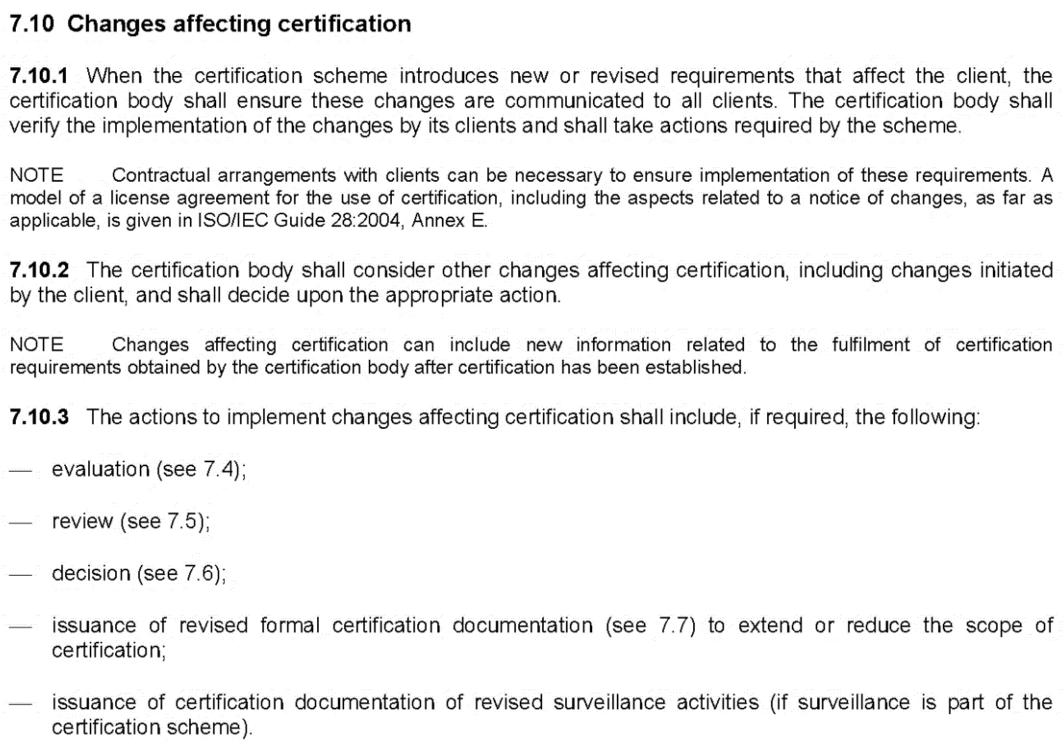
The full life cycle of a certificate, starting from its issuance with a defined validity period till its due or potential expiration (by validity period or preliminary to this due to a selection under the sampling rules for the general monitoring of certificates, a potential or actual non-conformity with security requirements, or an identified non-compliance with the accreditation requirements of the CAB, the CSA provisions, or the scheme requirements) has been considered.

One fundamental condition for issuing a certificate for the ICT product is successful evaluation, based on the CEM. Other conditions stem from relevant provisions of the CSA, such as necessary authorizations for CAB based on Article 60.3 of the CSA which are external to the certification in its technical meaning, and may, if not fulfilled after certification, be considered as non-conformance cases.

All other certification activities are related to the phase after the certificate is issued, where ‘*a change affecting certification*’ occurs as mentioned in ISO/IEC 17065. These activities are described as ‘maintenance’. In that case, the CB is obliged to act in response to a given trigger.

Wording from ISO/IEC 17065 describing all relevant activities related to the certificate which has been issued applies (see Clause 7.10):

Figure 3: Changes affecting certification (excerpt form ISO/IEC 17065)



7.10 Changes affecting certification

7.10.1 When the certification scheme introduces new or revised requirements that affect the client, the certification body shall ensure these changes are communicated to all clients. The certification body shall verify the implementation of the changes by its clients and shall take actions required by the scheme.

NOTE Contractual arrangements with clients can be necessary to ensure implementation of these requirements. A model of a license agreement for the use of certification, including the aspects related to a notice of changes, as far as applicable, is given in ISO/IEC Guide 28:2004, Annex E.

7.10.2 The certification body shall consider other changes affecting certification, including changes initiated by the client, and shall decide upon the appropriate action.

NOTE Changes affecting certification can include new information related to the fulfilment of certification requirements obtained by the certification body after certification has been established.

7.10.3 The actions to implement changes affecting certification shall include, if required, the following:

— evaluation (see 7.4);

— review (see 7.5);

— decision (see 7.6);

— issuance of revised formal certification documentation (see 7.7) to extend or reduce the scope of certification;

— issuance of certification documentation of revised surveillance activities (if surveillance is part of the certification scheme).

13. RULES RELATED TO NON-COMPLIANCE

REFERENCE ARTICLE(S) OF THE CSA

Article 54.1. *A European cybersecurity certification scheme shall include at least the following elements:*

l) rules concerning the consequences for ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme.

Article 56.8. *The holder of a European cybersecurity certificate shall inform the authority or body referred to in paragraph 7 of any subsequently detected vulnerabilities or irregularities concerning the security of the certified ICT product, ICT service or ICT process that may have an impact on its compliance with the requirements related to the certification. That authority or body shall forward that information without undue delay to the national cybersecurity certification authority concerned.*

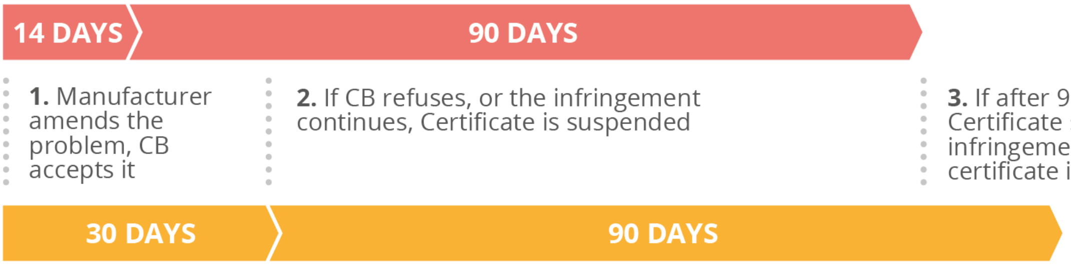
Without prejudice to NCCA activities defined under Articles 58.7 and 58.8 of the CSA and presented in Chapter 11, RULES FOR MONITORING COMPLIANCE, the consequences for ICT products that have been certified but which do not comply with the requirements of the scheme shall be, in line with the cases defined under Chapter 11, RULES FOR MONITORING COMPLIANCE, as follows.

Consequences vary according to the assessed non-conformities and non-compliances. Certificate suspension is introduced as to allow the necessary changes and/or controls to occur.

For confirmed deviations or irregularities associated to a non-compliance in the application by a manufacturer or provider of the requirements related to a certificate issued on their ICT product, the following consequences shall be in the general case:

- the CAB issuing the certificate shall request the manufacturer or provider for assertions and amendments to be provided within the time frame of 14 days/30 days for certificates at the assurance level 'high' /'substantial' of the CSA, in order to restore compliance;
- the CAB shall review the provided assertions and amendments and accept or refuse them; the decision shall be sent to the manufacturer or provider;
- continued infringements of such obligations shall trigger certificate suspension of the certificate for the ICT product and temporal suspension of certificate applications to the CAB by the manufacturer or provider, with an information from the CAB to the NCCA;
- when the handling is refused, or the suspension reaches a 90 day period the certificate shall be withdrawn.

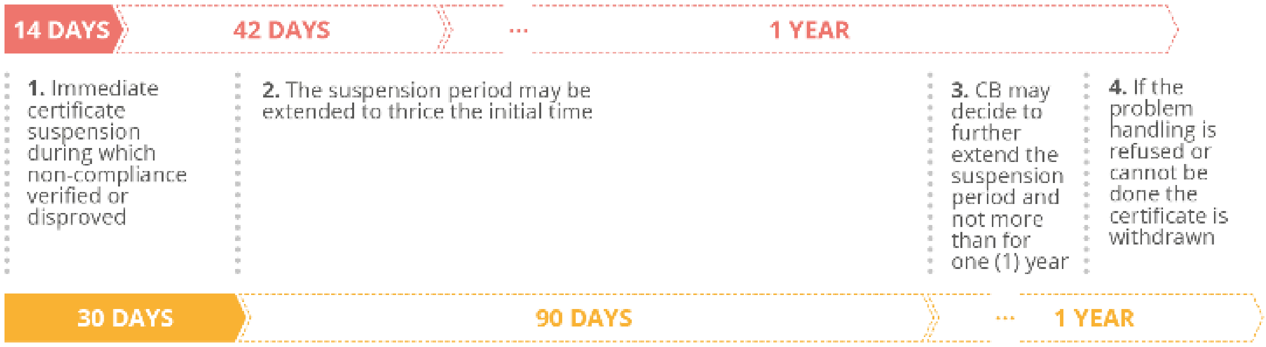
Figure 4: Timelines of non-compliance handling in the application of the requirements related to a certificate


14 DAYS
90 DAYS
1. Manufacturer amends the problem, CB accepts it
2. If CB refuses, or the infringement continues, Certificate is suspended
3. If after 90 days of Certificate suspension the infringement still persists, certificate is withdrawn
30 DAYS
90 DAYS

In the particular case of a confirmed deviation from the requirements on the certificate holder's obligations towards maintaining the certificate validity, or towards informing the appropriate authorities or bodies of any subsequently detected vulnerabilities, as requested by Article 56.8 of the CSA:

- an immediate certificate suspension shall occur starting at the notification of the owner of the certificate by the issuer of the certificate, with a maximum suspension period of 14 days/30 days for certificates at the assurance level 'high' /'substantial' of the CSA;
- during this period:
  - the non-compliance shall be verified or disproved with the necessary support[21] of the manufacturer or provider;
  - when the non-compliance is verified to impact a certificate, this shall be treated as a non-conformity of the certified ICT product;
  - the manufacturer or provider of the ICT product shall accept or refuse the handling of the verified product-related non-conformity and the necessary maintenance activities, as defined by Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES; when the defined period is not sufficient for the above described task, the issuer of the certificate upon receiving a justified request may extend the suspension period, no more than three times the above described length;
- when the handling is refused, the certificate shall be withdrawn;
- when the handling is accepted, the manufacturer or provider shall proceed to the necessary changes to the ICT product and the CB to related modifications of the status of the certificate;
- depending on the technical character and the emergency of the changes, the CB shall decide whether the changes are handled according to the requirements established in Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES or to the patch management solution defined under Chapter 14, RULES RELATED TO HANDLING VULNERABILITIES;
- where necessary (e.g. lack of availability of the CB), the CB may decide to further extend the suspension period for not more than one (1) year.

Figure 5: Timelines of non-compliance handling in case of a confirmed deviation from the requirements on the certificate holder's obligations towards maintaining the certificate validity, or towards informing the appropriate authorities or bodies of any subsequently detected vulnerabilities.


14 DAYS
42 DAYS
...
1 YEAR
1. Immediate certificate suspension during which non-compliance verified or disproved
2. The suspension period may be extended to thrice the initial time
3. CB may decide to further extend the suspension period and not more than for one (1) year
4. If the problem handling is refused or cannot be done the certificate is withdrawn
30 DAYS
90 DAYS
...
1 YEAR

At the beginning of the suspension period, the owner of the certificate shall be informed about the length of the period, the reason for the suspension and possible consequences. The suspension status of the certificate shall be notified to the NCCA and disclosed to ENISA for publication on its website.

For a confirmed non-compliance in the conditions under which the certification takes place and that are not related to an individual ICT product, the concerned CB shall proceed, under the control of its NCCA, to the following:

- the identification, with the support[22] of the concerned ITSEF, of potentially impacted certified ICT products;
- where deemed necessary by the CB, or at the discretion of the NCCA, the request for a series of evaluation tasks to be performed on one or more products by either the ITSEF which performed the evaluation, or any other ITSEF that would be in a better technical position to support that identification;

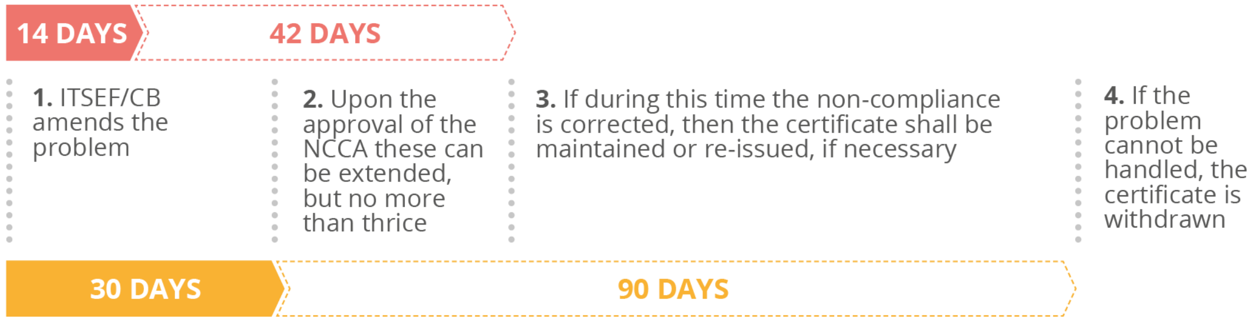
[21] Where necessary, support shall imply financial support to described activities.
[22] Where necessary, support shall imply financial support to described activities.

- the analysis by the CB of related evaluation reports, and where necessary, the re-emission of certificates in accordance with the requirements of Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES or the notification to the manufacturers of providers of the products of the impacts of the non-compliance on their certificates.

These activities shall occur within the maximum period of 14 days/30 days for certificates at the assurance level 'high' /'substantial' of the CSA, that may only be extended with the approval of the NCCA, but no more than three times the above described length. If during this time the non-compliance is corrected, then the certificate shall be either continued, renewed or re-issued, in accordance with Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES. If the problems cannot be handled, the certificate shall be withdrawn.

Where a CB or the NCCA mandates new evaluation activities to be performed, they shall be supported[23] by the CB or the ITSEF that proved not being compliant.

Figure 6: Timelines of non-compliance handling in the conditions under which the certification takes place

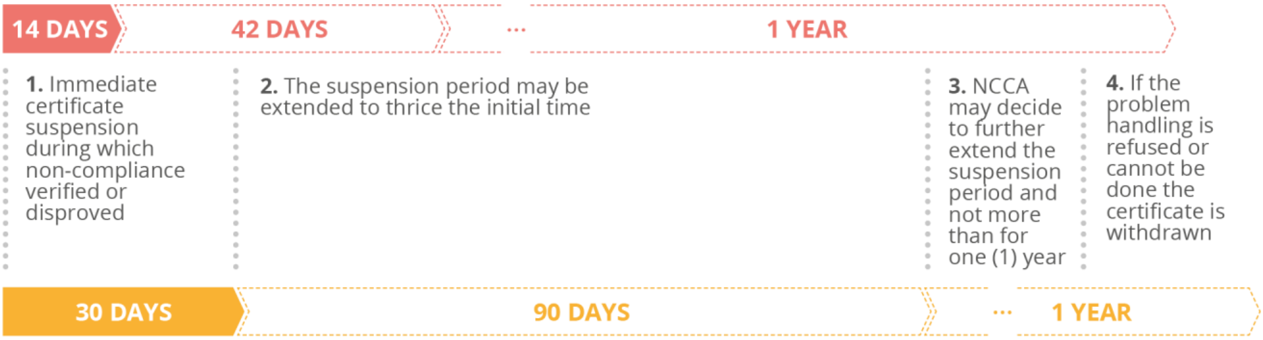

14 DAYS
42 DAYS
1. ITSEF/CB amends the problem
2. Upon the approval of the NCCA these can be extended, but no more than thrice
3. If during this time the non-compliance is corrected, then the certificate shall be maintained or re-issued, if necessary
4. If the problem cannot be handled, the certificate is withdrawn
30 DAYS
90 DAYS

Where impacts are confirmed to affect the validity of a certificate, they shall be treated as a non-conformity of the certified ICT product:

- an immediate certificate suspension shall occur starting at the notification of the owner of the certificate by the issuer of the certificate, with a maximum suspension period of 14 days/30 days for certificates at the assurance level 'high' /'substantial' of the CSA;
- during this period:
  - the manufacturer or provider of the ICT product shall accept or refuse the handling of the verified product-related impacts; when the defined period is not sufficient for the above described task, the NCCA upon receiving a justified request may extend the suspension period, no more than three times the above described length;
- when the handling is refused, the certificate shall be withdrawn;
- when the handling is accepted, the manufacturer or provider shall proceed to the necessary changes to the ICT product and the CB to related modifications of the status of the certificate;
- depending on the technical character and the emergency of the changes, the CB shall decide whether the changes are handled according to the requirements established in Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES or to the patch management solution defined under Chapter 14, RULES RELATED TO HANDLING VULNERABILITIES;
- where necessary (e.g. lack of availability of the CB), the NCCA may decide to further extend the suspension period, but not more than for a year.

[23] Where necessary, support shall imply financial support to described activities.

Figure 7: Timelines of non-compliance handling in the conditions under which the certification takes place and where impacts are confirmed to affect the validity of a certificate


14 DAYS
42 DAYS
...
1 YEAR
1. Immediate certificate suspension during which non-compliance verified or disproved
2. The suspension period may be extended to thrice the initial time
3. NCCA may decide to further extend the suspension period and not more than for one (1) year
4. If the problem handling is refused or cannot be done the certificate is withdrawn
30 DAYS
90 DAYS
...
1 YEAR

The consequences of confirmed non-compliances in the conditions under which the certification takes place and that are not related to the individual ICT product shall be reported by the NCCA to the ECCG.

Where consequences are associated with previously undetected vulnerabilities, they shall be handled in line with the requirements established under Chapter 14, RULES RELATED TO HANDLING VULNERABILITIES.

Where a certificate is withdrawn by the issuer of the certificate, this shall be done in accordance with the conditions defined in Article 58.8.(e) of the CSA for certificates established at the assurance level ‘high’ of the CSA.

The promotion by the manufacturers or providers of certificates that have been suspended or withdrawn for their ICT products shall not be allowed.

BACKGROUND INFORMATION

Consequences for ICT products that have been certified but which do not comply with the requirements of the scheme, are defined according to the non-compliance cases established under Chapter 11, RULES FOR MONITORING COMPLIANCE. They take also into consideration the obligations of Article 56.8: “*The holder of a European cybersecurity certificate shall inform the authority or body referred to in paragraph 7 of any subsequently detected vulnerabilities*”.

The status of suspension for certificates is introduced as to allow the necessary analysis of impacts of assessed failures, before any other action related to changing the status of the certificate is decided, in accordance with the rules of Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES.

Where necessary, such analysis may require the necessary support of the issuers of certificates and their testing laboratories and/or of the holders of certificates.

Temporal suspension or reduction of certificate application for the product or by the developer has been introduced on repeated infringements of scheme obligations by a developer: a CAB may suspend or reduce the developer’s access to the scheme’s certification activities until sufficient evidence for the developer’s compliance has been reestablished by a CAB and confirmed by the NCCA.

Consequences of non-compliance in the conditions under which the certification takes place and that are not related to the individual ICT product are defined here for the concerned certificates. Consequences on the CAB and their testing laboratories are not defined here, and should be considered under the NCCA responsibilities to supervise their activities, as defined by Article 58 of the CSA.

Rules regarding the handling of previously undetected vulnerabilities are defined in Chapter 14, RULES RELATED TO HANDLING VULNERABILITIES and are not repeated here.

14. RULES RELATED TO HANDLING VULNERABILITIES

REFERENCE ARTICLE(S) OF THE CSA

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

m) rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with.

Article 55 .1. *The manufacturer or provider of certified ICT products, ICT services or ICT processes or of ICT products, ICT services and ICT processes for which an EU statement of conformity has been issued shall make publicly available the following supplementary cybersecurity information*:

(c) contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers;

(d) a reference to online repositories listing publicly disclosed vulnerabilities related to the ICT product, ICT service or ICT process and to any relevant cybersecurity advisories.

Article 56.8. *The holder of a European cybersecurity certificate shall inform the authority or body referred to in paragraph 7 of any subsequently detected vulnerabilities or irregularities concerning the security of the certified ICT product, ICT service or ICT process that may have an impact on its compliance with the requirements related to the certification. That authority or body shall forward that information without undue delay to the national cybersecurity certification authority concerned.*

Previously undetected vulnerability shall be reported and handled in accordance with the general rules of ISO/IEC 30111 and ISO/IEC 29147, adapted for this scheme, with the additional possibility of patch management

Vulnerability handling

Manufacturers or providers of ICT products shall use the general steps of ISO/IEC 30111 for vulnerability handling: preparation, receipt, verification, remediation development, release, post release, with the following specific application rules for the EUCC scheme.

1 PREPARATION

Manufacturers or providers of ICT products shall develop methods for receiving vulnerability information and make them public in accordance with Article 55.1.c) of the CSA.

2 RECEIPT

In the following cases where:

- the manufacturer or provider of the ICT certified product receives vulnerability information according to Article 55.1.(c) of the CSA;
- there is a new publicly disclosed vulnerability on the referenced online repositories according to Article 55.1.(d) of the CSA;
- the manufacturer or provider finds out a related vulnerability to its ICT certified product in any other way,

the manufacturer or provider shall report within a business day to the certification body (CB) that issued the certificate the possibility of a related vulnerability and provide within five business days a date for when a vulnerability analysis will be established.

When the information about a possibility of a vulnerability related to the certified ICT product is available first at the CB, the CB shall inform within a business day the manufacturer or provider and request a vulnerability analysis and a date for this analysis within five business days.

The CB shall agree on the proposed date, but this shall not exceed 90 days. When both parties deem necessary or are unable to agree on such a date, they may inform the NCCA and ask for its advice they may ask the NCCA for its advice.

The certificate shall be suspended in the following cases where the manufacturer or provider fails to:

- inform the CB within the agreed date;
- provide the vulnerability analysis within the agreed date;
- answer the request of the CB within a previously agreed time period e.g. within five business days.

3 VERIFICATION

The vulnerability analysis shall be documented, and the documentation kept for at least five years by all parties.

It shall contain Attack Potential Calculation according to Chapter 3 EVALUATION STANDARDS, which may be reviewed by the ITSEF. This Attack Potential Calculation shall aid the decision whether the vulnerability is residual or exploitable at the selected AVA_VAN level for the certificate.

It shall indicate whether the vulnerability is disproved or confirmed for the certified ICT product.

Where necessary, the manufacturer or provider may ask for more information from the information source(s), before the calculation is concluded.

In the case the vulnerability is disproved, the process shall stop and the information be kept for any further investigation.

In the case the vulnerability is confirmed and applies to the product, the following paragraphs shall apply.

The vulnerability analysis shall contain the impact assessment on the ICT product and possible resolution(s) of the vulnerability, with the following information:

- possible risks associated to the proximity or availability of the possible attack;
- level of the changes which will need to apply, in accordance with Annex 11, ASSURANCE CONTINUITY.

The information may contain details about the possible exploit(s) of the vulnerability: in that case, it shall carry the appropriate TLP classification as to ensure the relevant protection, in accordance with the standard rules defined in https://www.first.org/tlp/.

Alternatively to TLP classification ANNEX 2 MSSR 9.1.3 Classification of information, data, and material may be applied. ISO 29147 also lists TLS, S/MIME and PGP as typical security mechanisms may also be considered

The analysis shall be shall be sent to, and approved by the CB and may lead to the conclusion that the vulnerability cannot be circumvented. In that case, the certificate shall be withdrawn. If the analysis concludes that the vulnerability can be patched, then the certificate shall be suspended and the following shall be applied.

The CB shall inform the NCCA of a verfiied vulnerability information.

The monitoring of valid certificates by the NCCA shall take into account the backlog of such vulnerability analysis for the sampling of certificates to be re-assessed.

4 REMEDIATION DEVELOPMENT

The certified ICT product may include a patch management mechanism, as defined in Annex 15, PATCH MANAGEMENT which is for trial use[24], that was assessed within its certification: associated conditions shall then apply.

Where the certified ICT product does not include such a patch management mechanism, the maintenance process described in Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES and associated activities defined in Annex 11, ASSURANCE CONTINUITY shall be applied to verify the correctness of the changes made to cover the vulnerability, and to reissue any necessary updated certificate.

In either case, the manufacturer or provider shall make the decision on remediation and produce the necessary changes to the ICT product that shall be tested in accordance with Annex 15 or Annex 11. Non-regression testing shall also be performed to ensure the further ability to introduce a new patch.

[24] As defined in Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS.

5 RELEASE AND POST RELEASE

Where remediation and associated changes to the ICT product have been declared apt for deployment, the manufacturer or provider shall directly proceed to their deployment or proceed to their release in accordance with the requirements of Article 55.1.(d) of the CSA.

The security lifecycle of the ICT product shall in addition be updated, based on the root cause analysis of the vulnerability.

Vulnerability disclosure

Manufacturers or providers of ICT products may use the following standard as for the general rules related to vulnerability disclosure:

- ISO/IEC 29147 Information technology - Security techniques - Vulnerability disclosure.

During the vulnerability analysis, the manufacturer may apply an embargo period, meaning that the possible vulnerability is not further disclosed. This period shall not last longer than one (1) month. The NCCA may, however, consider extending this period when a justified request is received, in particular when it is confirmed that time must be given to downstream vendors integrating the product or service for analysing the impact of the vulnerability (both from a technical and certification point of view).

In addition to the general disclosure rules above, once a strategy to correct the issue has been defined by the manufacturer or provider with the approval of the CB, or as soon as the decision was taken that the vulnerability could not be mitigated, information related to the confirmed vulnerability shall be disclosed to the NCCA, in accordance with Article 56.8) of the CSA.

The information shall not contain details about the possible exploit of the vulnerability. It shall contain the necessary elements for the NCCA to understand the impact of the vulnerability, the changes to be brought to the product, and where applicable, information by the CB on the broader applicability of the vulnerability to other certified products.

The NCCA shall in accordance with Art.icle 58 7 h) share this information with the other NCCAs, which may also decide to further analyse the problem or, after informing the manufacturer or provider of the ICT product about the information exchange, ask the related CABs to analyse whether further certified products are affected. This information exchange shall be done in confidentiality (encrypted).

When a correction has been brought to the certified product, the manufacturer or provider shall establish the necessary CVE with the support of the NCCA and related national CSIRT, and proceed to its publication on the relevant list, in accordance with the requirements of Article 55 of the CSA. ENISA shall be informed of the changes of status of the related certificates.

NCCAs may develop their capacity to act as “coordinators” as defined in ISO/IEC 29147, and alternatively, designate their national CSIRT to play this role. In that case, the CSIRT shall have access to the necessary details related to the vulnerabilities and to the certificated ICT products.

BACKGROUND INFORMATION

The EUCC Scheme vulnerability handling and disclosure processes are based on the ISO standards ISO/IEC 30111 and ISO/IEC 29147. However, as these standards do not contain any assurance on whether the developed and deployed remediation does not introduce new vulnerabilities, and do not define any tasks for a third-party assessment body and its methodology, additional information was provided into this chapter as well as in the Chapter 15, PATCH MANAGEMENT, to cover these gaps.

Beside the already accepted methodologies described in Annex 11, the EUCC Scheme also adds new handling methods for the vulnerability and disclosure processes and patch management.

The following figure gives an overview of the process:

Figure 8: Vulnerability handling and disclosure processes

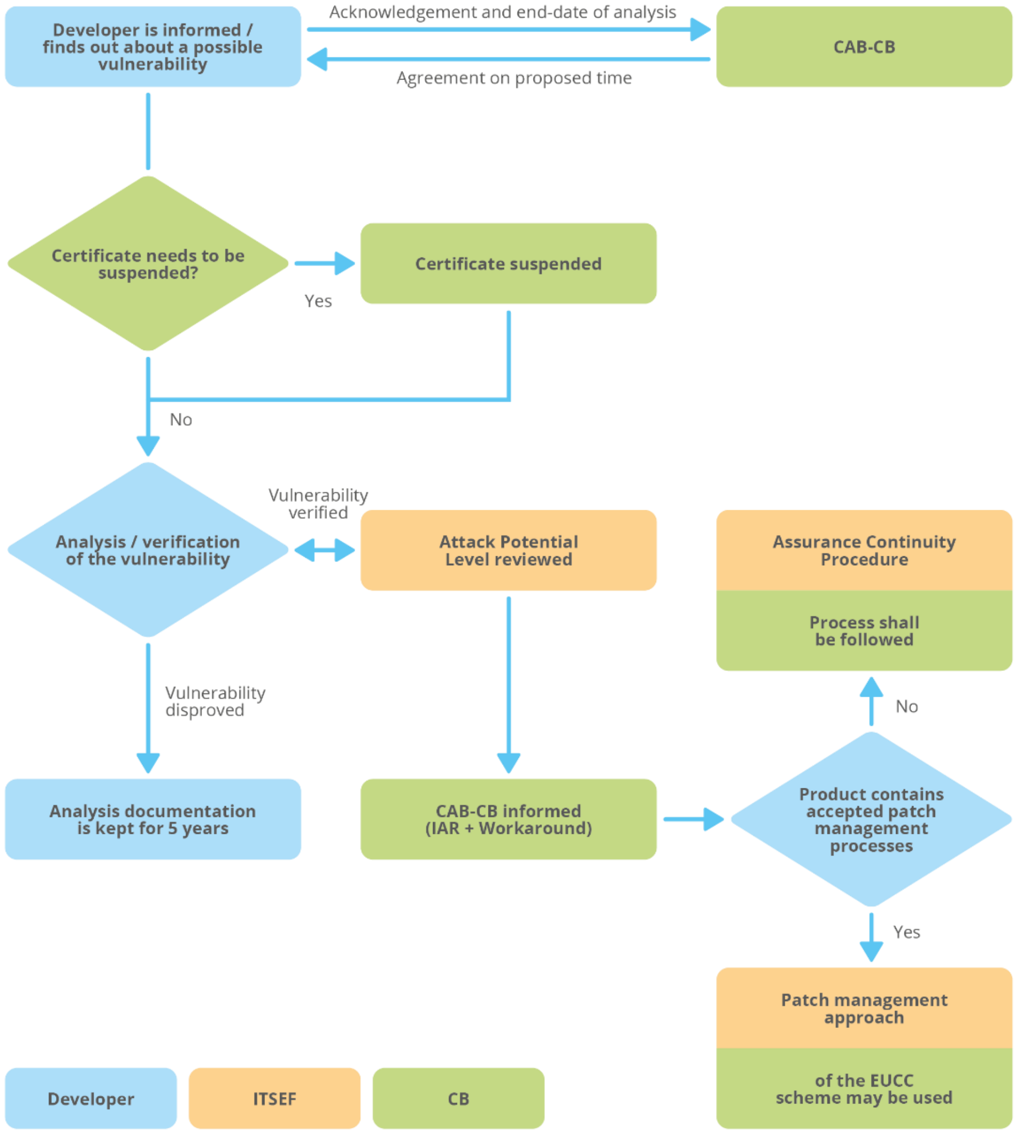
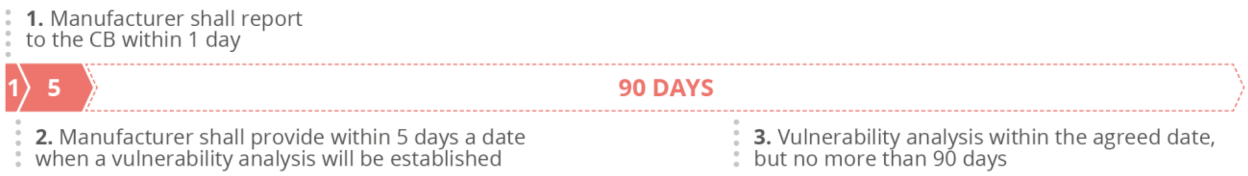

Developer is informed / finds out about a possible vulnerability
Acknowledgement and end-date of analysis
Agreement on proposed time
CAB-CB
Certificate needs to be suspended?
Yes
Certificate suspended
No
Analysis / verification of the vulnerability
Vulnerability verified
Attack Potential Level reviewed
Assurance Continuity Procedure
Process shall be followed
Vulnerability disproved
No
Analysis documentation is kept for 5 years
CAB-CB informed (IAR + Workaround)
Product contains accepted patch management processes
Yes
Patch management approach
of the EUCC scheme may be used
Developer
ITSEF
CB

Figure 9: Timeline of the general vulnerability handling


1. Manufacturer shall report to the CB within 1 day
1
5
90 DAYS
2. Manufacturer shall provide within 5 days a date when a vulnerability analysis will be established
3. Vulnerability analysis within the agreed date, but no more than 90 days

15. RETENTION OF RECORDS BY A CAB

REFERENCE ARTICLE(S) OF THE CSA

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

n) where applicable, rules concerning the retention of records by conformity assessment bodies.

Retention of records by CAB shall follow the general rules of accreditation standards ISO/IEC 17065 and ISO/IEC 17025.

Each CAB shall maintain a record system in accordance with the requirements of the applicable accreditation standard ISO/IEC 17065 or ISO/IEC 17025 for its activity.

The record system shall include all records and other documents produced in connection with each certification; it shall be sufficiently complete to enable the course of each certification to be traced.

All records shall be securely and accessibly stored for a period of at least five (5) years after the expiration date of the certificate.

In case a different expiration date of the certificate has been attributed in accordance with the conditions of Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES, it shall be taken into account for the new calculation of the retention period of the records, with the same rule as previously stated. New or revised information related to the activities described under Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES shall be added to the previous records for the certificate.

BACKGROUND INFORMATION

The standards ISO/IEC 17065 and ISO/IEC 17025 already provision requirements related to the retention of records during the whole validity period of the certificate. In order to be able to manage potential commercial disputes, it is recommended to extend the retention period after the expiration date of the certificate. An additional period on five (5) years is a current common practice.

Maintenance, recertification and reassessment process by the CAB may change the expiration date of a certificate. This new expiration date has to be applied to retention of the records produced within this process. As the certificate validity may not be a fixed value, it has been recommended to set a requirement after the expiration of the certificate, in order to be able to manage potential commercial disputes.

16. NATIONAL OR INTERNATIONAL SCHEMES

REFERENCE ARTICLE(S) OF THE CSA

Article 1.2. *This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the State in areas of criminal law.*

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

> *o) the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services and ICT processes, security requirements, evaluation criteria and methods, and assurance levels.*

Article 57 1. *Without prejudice to paragraph 3 of this Article, national cybersecurity certification schemes, and the related procedures for the ICT products, ICT services and ICT processes that are covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant to Article 49(7). National cybersecurity certification schemes and the related procedures for the ICT products, ICT services and ICT processes that are not covered by a European cybersecurity certification scheme shall continue to exist.*

Article 57 3. *Existing certificates that were issued under national cybersecurity certification schemes and are covered by a European cybersecurity certification scheme shall remain valid until their expiry date.*

Some EU schemes participating to the SOG-IS MRA cover the same type or categories of ICT products, but may go beyond the EUCC in terms of national certification, or cover partly the EUCC assurance levels.

Following Common Criteria based certification schemes cover the same type or category of ICT products, security requirements, evaluation criteria and methods, and assurance levels:

Within the EU, the:

- French scheme, operated by ANSSI: https://www.ssi.gouv.fr/administration/produits-certifies/cc/
- German scheme, operated by BSI: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/zertifizierungnachcc_node.html
- Italian scheme, operated by OCSI: www.ocsi.isticom.it/
- Dutch scheme, operated by TÜV Rheinland NL and NLNCSA: http://www.tuv-nederland.nl/nl/17/common_criteria.html
- Spanish scheme, operated by CCN: https://oc.ccn.cni.es/
- Swedish scheme, operated by FMV: http://fmv.se/en/Our-activities/CSEC---The-Swedish-Certification-Body-for-IT-Security/

European Economic Area (EEA) European Free Trade Association (EFTA) States, the:

- Norwegian scheme, operated by SERTIT: http://www.sertit.no/

Some of these schemes may not currently cover all Technical Domains defined under Chapter 4, ASSURANCE LEVELS. This information may be retrieved from the SOG-IS MRA following page: https://www.sogis.eu/uk/status_participant_en.html

Considering the possibility that a:

- certificate issued under these schemes could where necessary[25] be transformed into a certificate under the EUCC scheme if necessary activities are conducted;
- CB may accept to reuse the results of evaluations activities performed under these schemes for a certification under the EUCC scheme;
- certificate issued under these schemes may be reused for composite certifications under the EUCC scheme until its period of validity, if evaluation work confirms that the composed ICT product meets all requirements of the EUCC scheme;

ENISA may establish associated guidance as to support the conditions associated to these possibilities, as defined under Chapter 25, RECOMMENDATIONS FROM THE AHWG. This guidance shall be established in cooperation with the ECCG.

Based on the recommendations established by this Chapter, the European Commission and EU Member States may consider to establish a date of two (2) years after the implementing act has been adopted pursuant to Article 49(7) for existing schemes to cease producing effect.

Some of these schemes may run certification activities covering the same type or category of ICT products, security requirements, evaluation criteria and methods and go beyond the scope of the EUCC scheme in terms of assurance levels (e.g. where no Technical Domain/no specific Protection Profile for this purpose has been yet defined/annexed for the EUCC scheme for certificates associated to AVA_VAN.4 or 5).

Associated certificates shall not be issued under the EUCC scheme.

The following international schemes participating to the CCRA cover the same type or category of ICT products, security requirements, evaluation criteria and methods, and may not address all assurance levels of the EUCC scheme: https://www.commoncriteriaportal.org/ccra/schemes/?CFID=50893710&CFTOKEN=ccb21e6bbf0ccebe-BBE1E229-155D-00D0-0A23555C0903C74A

BACKGROUND INFORMATION

The use of existing schemes installed for ICT product certification using the Common Criteria should remain possible for certifications that would fall out of the scope of the EUCC scheme, be it for other purposes (e.g. national security) or beyond the conditions of the scheme (e.g. a AVA_VAN.4 or 5 certificate for an ICT product not covered by a Technical Domain nor a specific Protection Profile attached to this scheme, such as a pure software product). Such certificates should not carry out the recognition mark or label of the EUCC scheme.

Apart from these specific cases, and in order to benefit from the combined advantages of Common Criteria and EUCC certification, risk owners needing Common Criteria certification for ICT products are advised to make use of the following requirements for these ICT products, or equivalent: “The Common Criteria certification of the [ICT product] shall be performed according to the EUCC scheme, or to a SOG-IS CC scheme operated by one of the EU member states if the certificate is scheduled for delivery prior to the moment when the EUCC scheme will start delivering certificates.“

If the ICT product is certified by a MS SOG-IS scheme before the EUCC scheme starts producing effect, the risk owner may consider the additional requirement that an application for a EUCC certificate of the SOG-IS certified product be done when the EUCC scheme starts operating. Indeed, this is the stated goal of this scheme to ensure efficient conversion of a SOG-IS MRA certificate.

Converting a SOG-IS MRA certificate to the EUCC scheme and reusing certificates for composition allow for efficient reuse of existing certificates, this will require guidance as to address in a harmonised way the differences between the old and the new schemes.

On certificates used for composition: the preferred solution should be that certificates used for composition are converted in the new scheme. However, when it is not done for any given reason that can be dealt with at composition product level (eg: availability of supplementary cybersecurity information as required by Article 55 of the CSA, content and format of the certificate…) it is worth having a backup solution where the composed ICT product can “carry the weight” of the necessary improvements to reach the requirements of the EUCC scheme.

[25] To satisfy market or regulatory requirements.

17. CONTENT AND FORMAT OF CERTIFICATES

REFERENCE ARTICLE(S) OF THE CSA

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

> *p) the content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued.*

A certificate contains the most relevant information for the identification of the product and the assurance level obtained.
It provides easy access to Supplementary cybersecurity information and will include a label when available.

A certificate shall at least include at the following information:

- a unique identifier established by the issuer of the certificate;
- information related to the certified ICT product and its manufacturer or provider:
    - name of the ICT product, and where applicable of the TOE;
    - type of the ICT product, and where applicable of the TOE;
    - version for the ICT product;
    - name and contact information of the manufacturer or provider;
    - link to the website of the manufacturer or provider to access the Supplementary cybersecurity information for the certified ICT product in accordance with Article 55 of the CSA;
- information related to the evaluation and certification of the ICT product:
    - name and contact information of the body or authority that issued the certificate;
    - name of the ITSEF which performed the evaluation, when different from the certification body;
    - name of the responsible NCCA;
    - reference to this scheme;
    - reference to the certification report associated with the certificate;
    - assurance level from the CSA reached (either ‘substantial’ or ‘high’);
    - CC version/release used for the evaluation;
    - identification of the assurance level or package from the CC, including used assurance components and AVA_VAN level covered;
    - where applicable, reference to Protection Profile(s) to which the ICT product complies;
    - date of issuance and period of validity of the certificate;
- when available, the mark of label associated to the scheme, as defined by Chapter 10, MARKS AND LABELS.

Where the certified part of the ICT product (the TOE) significantly differs from the ICT product, a clear indication shall be given on the perimeter of the TOE into the information related to the certificated ICT product; where applicable, the TOE may therefore be identified by a specific name related to its dedicated functionality within the ICT product and a specific type.

ENISA may provide, in cooperation with the ECCG, guidance as how to determine unique identifiers in order to ease the access of users to the history of the certificates associated to a product and its different versions.

Where applicable, the assurance package shall distinguish between CC Part 3 Evaluation Assurance Level conformant and CC Evaluation Assurance Level Part 3 augmented, in accordance with the conditions defined in Annex 1.

ENISA may provide in cooperation with the ECCG guidance on taxonomy of ICT products, as to offer a harmonised list of types of ICT products across the EU. When such taxonomy has been established:

- the CAB shall assess to which type the certificates refers to;

- NCCA may define which particular types may benefit from a potential extension of the period of validity of associated certificates, as defined by Chapter 19, PERIOD OF VALIDITY OF CERTIFICATES.

Each certificate shall be signed by the appropriate responsible person of the authority or body and made available to the NCCA and to ENISA with its associated certification report in electronic form and in English language. In case such documents are produced in a language different from English, a courtesy translation shall be provided.

When a label has been established for the scheme, ENISA may attribute a QR code in association to the label into the certificate. This QR code may be used with the label by the manufacturer or provider in the documentation or packaging associated to a certified ICT product.

For each certificate, a certification report shall be established by the issuer of the certificate. It shall at least contain the information detailed in Annex 13, and shall contain the following disclaimer:

The certification or certificate is entirely related to the cybersecurity certification requirements of the product at the moment of issuance of the certificate. It is not related to the product itself.
The certification is not an endorsement of the product, the package or anything else related to the product, It only expresses that the cybersecurity related material and information of the product meets the requirements of this certification related information. There are no warranties about fit for purpose or merchantability, absence of defects, errors, accuracy, non-infringement of intellectual property rights, consumer rights and any other related rights. The issuer of the certification or the cybersecurity certification scheme owner are under no circumstances liable for any direct, indirect, material, technical and IT functionality related or moral damages of any kind arising out of the product for non-use, or use.
Neither will any loss of goodwill, work stoppage, computer failure or malfunction, loss or damages, amendments, misuse, abuse, alteration, destruction, theft, ransom or any other form of unauthorised access to data or any commercial damage generate liability to the issuer of the certificate or the designer of the certification scheme or any other organisation that recognises or gives effect to this certificate, except for gross negligence or wilful misconduct caused by natural persons working under these institutions.

BACKGROUND INFORMATION

The content of the EUCC certificates inherits from the content of SOG-IS MRA certificates and also includes the necessary information related to the new scheme, such as a link to the Supplementary cybersecurity information in accordance with Article 55 of the CSA, as well as the potential mark or label associated to the scheme.

The possibility for ENISA to issue QR codes associated to certificates should allow the manufacturer or provider, through the documentation or packaging associated to a certified product, to facilitate the access to the ENISA website where certificates are displayed.

As a certificate cannot encompass all relevant information associated with the certified product, a certification report that contains more detailed information shall be established and published in association with the certificate.

18. AVAILABILITY OF INFORMATION

REFERENCE ARTICLE(S) OF THE CSA

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

> *q) the period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services or ICT processes.*

Information associated to a certified ICT product shall be available for a period of at least five years after the expiration date of the certificate.

Each manufacturer or provider of ICT products shall maintain a publication system for the information to be made available to the public, in accordance with the procedures described in Chapter 23, SUPPLEMENTARY CYBERSECURITY INFORMATION - ARTICLE 55 for the Supplementary cybersecurity information.

All information shall be available for a period of at least five (5) years after the expiration date of the certificate.

In case a different expiration date of the certificate has been attributed in accordance with the activities described under Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES, it shall be taken into account for the calculation of the availability period of the information, with the same rule as previously stated.

Available information shall be updated with the new or revised information related to the activities performed under Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES.

Records of information delivered to the CAB for the certification process, as well as samples of the version of the certified ICT product, shall be stored securely, and made available on its request to the CAB or the NCCA (according to Article 58.8(a) of the CSA) up to five years after expiration of the certification, in line with the duration established under Chapter 15, RETENTION OF RECORDS BY A CAB.

BACKGROUND INFORMATION

The period of retention for manufacturers and providers of ICT products shall not be shorter than the retention of records by the CAB that is of five (5) years after the end of validity period of the certificate.

It is to be noted that manufacturers and providers may however have to extend this period, in order to comply with other regulations (e.g. EU No 305/2011[26], 2014/53/EU[27], 2014/35/EU[28], 2006/42/EC[29]) that state a different period of availability of documentation, up to ten (10) years.

When a certificate has to be modified, some of the information associated to the ICT product may be deprecated and replaced by new information, and the need to maintain available information on the ICT product only relates to the valid and up-to-date information. The deprecated information shall still be archived for ten (10) years, or for the duration of the related certificate plus five (5) years if this exceeds ten (10) years.

On the availability of information related to the certification: the availability of the certified version of the product at the manufacturer's or developer's level is requested for any further investigation that might be required, and as there is the assumption that this is something the CAB cannot afford on its own, for practical reasons.

[26] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011R0305.
[27] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0053.
[28] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0035.
[29] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0042.

19. PERIOD OF VALIDITY OF CERTIFICATES

REFERENCE ARTICLE(S) OF THE CSA

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

r) maximum period of validity of European cybersecurity certificates issued under the scheme.

The maximum period of validity of the certificates shall be five (5) years.

The maximum period of validity of the certificates shall be five (5) years.

Under certain conditions including the approval of its NCCA, and following the processes defined in Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES, a CAB may continue a certificate with an extended validity period beyond the initial five (5) years. Extended validity period certificates may be considered for sampling according to Chapter 11 RULES FOR MONITORING COMPLIANCE.

A shorter maximum period of validity may be specified within a specific Technical Domain, as defined by Chapter 4, ASSURANCE LEVELS.

BACKGROUND INFORMATION

According to the large variety of ICT products that can be certified under this scheme, to their different possible implementations (software, hardware…) and evolutions (frequent or rare updates), to the various levels of assurance that can be achieved and the associated effort to assess their robustness, according also to the conditions for their deployments and their life time, an average maximum of five (5) years was selected for the general case.

This period is also in line with the period defined under the CCRA[30].

The possibility, however, to go beyond this period of five (5) years has been established, and associated conditions defined under Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES (including a reassessment of the cybersecurity of related ICT products), in order to allow ICT products that are deployed for a longer period (such as passports) to be certified for the whole duration of their life-cycle.

On the other hand, the possibility to limit the maximum period has been introduced, as it may become a necessity for some specific ICT products: it is foreseen that this may occur for specific Technical Domains.

[30] https://www.commoncriteriaportal.org/products/ The CCDB has approved a resolution to limit the validity of mutually recognized CC certificates over time. Certificates will remain on the CPL for five years. Effective 1 June 2019, certificates with an expired validity period (that is, 5 years or more from the date of certificate issuance) will be moved to an Archive list on the CCRA portal, unless the validity period has been extended using the appropriate procedures.

20. DISCLOSURE POLICY FOR CERTIFICATES

REFERENCE ARTICLE(S) OF THE CSA

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

s) disclosure policy for European cybersecurity certificates issued, amended or withdrawn under the scheme.

ENISA will publish the certificates with appropriate relevant information attached. To manage accurate and up to date dataflows, ENISA will establish conditions and/or guidance for the delivery and publication of information.

The certificates shall be disclosed by ENISA, with the related certification report and any relevant information as requested by other chapters of this document, in a dedicated website on European cybersecurity certification schemes, in accordance with Article 50.1 of the CSA.

The certificates shall be disclosed with their applicable status, as deciced through the application of the requirements established by Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES and Chapter 13, RULES RELATED TO NON COMPLIANCE.

The certificates may also be disclosed by the NCCAs and related CBs on their websites. Any change to the status of a certificate shall be reported to ENISA.

Amendments and withdrawals of certificates resulting from maintenance activities shall as well be published, in a way that users of certificates can identify which versions of a certified ICT product are certified, which versions are no more certified and which relevant information shall apply (such as guidance).

ENISA shall establish in cooperation with the ECCG the conditions and/or guidance for the delivery and for the publication in due time of certificates and their updates, and associated relevant information, and shall make them publicly available on its Website dedicated to cybersecurity certification.

Such information on the Website on European cybersecurity certification schemes shall be available in English language. It shall be available at least for the entire period of validity of the certificate.

The certificates may be complemented with additional information, such as a QR-code providing a direct link to the corresponding security target (security target lite, if available) and product certificate, and (with the consent of manufacturers or providers) pictures of the certified ICT products, as to offer a better user experience and to publicise the certificates. ENISA may therefore establish a procedure for the generation of a QR-code: such procedure may imply that Certification Bodies (CB), ahead of the release of a certificate, request to ENISA the generation of the QR-code to be applied on the certificate and provided to the manufacturers or providers for their commercial and technical documents.

Only ICT products with a valid certificate shall be promoted as certified ICT products by their relevant manufacturer or provider, or users of these products.

Where Protection Profiles are certified under the conditions of this scheme, ENISA shall provide on its cybersecurity certification Website a list of these Protection Profiles.

BACKGROUND INFORMATION

In accordance with Chapter 17, CONTENT AND FORMAT OF CERTIFICATES, both certificates and associated certification reports, as well as relevant information for the secure configuration and usage of the certified ITC product (guidance) shall be made available to the users (and potential users) of certificates. Amendments to certificate will also need to contain the same type of information as the issuance of certificates, including guidance, and users shall be given an easy access to the status of the certificates when using ENISA dedicated Website.

As to offer an easy access to the Supplementary cybersecurity information defined by Article 55, a validated link to that information will be made available into the certificate.

ENISA shall be informed without undue delay of the evolution of the certificates, be it an amendment or a withdrawal, in line with the requirements of relevant Chapters of this scheme and Recital 93 of the CSA.

As to offer the necessary flexibility and enforcing character of the conditions for presentation of the information to ENISA, and for its publication, ENISA will establish generic conditions and/or guidance.

The generic conditions and/or guidance should make sure information is accurate and up to date as the information provided by ENISA could act as a single point of reference. It should define what information is to be transmitted to ENISA and within what reasonable timeframe. According to principles of transparency and openness, the outlines of these conditions/guidance should be made public on the ENISA Website.

As to promote valid certificates, certificates that have expired will be archived and made available on a different webpage than the valid ones.

21. MUTUAL RECOGNITION WITH THIRD COUNTRIES

REFERENCE ARTICLE(S) OF THE CSA

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

t) conditions for the mutual recognition of certification schemes with third countries.

The establishment of a mutual recognition agreement (MRA) between the participants shall support mutual recognition with third countries. Preliminary conditions for mutual recognition of certificates and for peer assessment are defined.

The mutual recognition of certification schemes with third countries shall be supported by the establishment of a Mutual Recognition Agreement (MRA) between the participants.

This MRA may include the following information:

- participants to the MRA;
- purpose and spirit of the Agreement;
- membership;
- scope;
- exceptions;
- definitions;
- conditions for recognition of certificates;
- peer assessments;
- publications;
- sharing of Information;
- acceptance of new participants and compliant authorities or bodies;
- administration of this Agreement;
- disagreements;
- costs of this Agreement;
- revision;
- duration;
- voluntary termination of participation;
- commencement and continuation;
- effect of this Agreement.

Conditions for recognition of certificates by participants to such an Agreement shall include at a minimum the following conditions:

- the participants shall commit themselves to recognise applicable conformant certificates by any accepted Participant;
- acceptance of participants shall confirm that the evaluation and certification processes have been carried out in a duly professional manner:
  - on the basis of commonly accepted ICT security evaluation criteria;
  - using commonly accepted ICT security evaluation methods;
  - in the context of an evaluation and certification scheme managed by a compliant certification body in the accepted participant's country;
  - the conformant certificates and certification reports issued satisfy the objectives of this Agreement;
- certificates which meet all these conditions shall be termed as conformant certificates for the purposes of this Agreement;
- ICT security evaluation criteria are to be those laid down in Chapter 3, EVALUATION STANDARDS of this document;
- minimum requirements for Certification Reports are laid down in Annex 13 to this document;
- the scheme of the participants or to which the participants adhere shall be organised with a proper National Authority, certification bodies (CBs) and testing laboratories (ITSEFs), in accordance with the following requirements:

  - the National Authority supervises the certification activities, notifies and authorises where applicable CB and ITSEF, and reports any vulnerability of certified ICT products to the NCCA of the EU participants;
  - the CB has been accredited in its respective country by a recognised Accreditation Body in accordance with ISO/IEC 17065 and has been authorised where necessary by the National Authority;
  - the CB is accepted as compliant by the Participants through a peer assessment mechanism installed for the MRA;
  - the ITSEF has been accredited in its respective country by a recognised Accreditation Body in accordance with ISO/IEC 17025 and where necessary subject to an assessment by the National Authority in order to confirm its competence to perform evaluations, in accordance with Chapter 6, SPECIFIC REQUIREMENTS APPLICABLE TO A CAB of this document;
- in order to assist the consistent application of the criteria and methods between evaluation and certification schemes, the participants plan to work towards a uniform interpretation of the currently applicable criteria and methods and commit to accept the supporting documents that results from this work. In pursuit of this goal, the participants also plan to conduct regular exchanges of information on interpretations and discussions necessary to resolve differences of interpretation;
- in further aid to the goal of consistent, credible and competent application of the criteria and methods, the certification bodies shall undertake the responsibility for the monitoring of all evaluations in progress within the MRA at an appropriate level, and carrying out other procedures to ensure that all ITSEFs affiliated with the CB:
  - perform evaluations impartially;
  - apply the criteria and methods correctly and consistently;
  - have and maintain the required technical competencies;
  - adequately protect the confidentiality of sensitive or protected information.

The MRA may include a limitation of the assurance level of the certificates subject to recognition.

CB(s) of the participants of such an Agreement that issue(s) certificates at the equivalent assurance level ‘high’ of the CSA shall be subject to peer assessments in line with the procedure set up in this scheme, in Annex 12.

The procedure may be adapted and simplified for the CBs that issue certificates at the equivalent assurance level ‘substantial’ of the CSA as to benefit from the international Accreditation system, and shall at least consist of the following activities by the peer assessment team regarding review of the:

- documentation associated to 2 certification projects of the ‘substantial’ assurance level;
- procedures associated to the security of information.

BACKGROUND INFORMATION

The establishment of a MRA may benefit from the experience of the existing MRA (CCRA and SOG-IS MRA), which define the conditions for participation and recognition of certificates, and do not both consider the same assurance levels for the recognition of certificates.

22. PEER ASSESSMENT

REFERENCE ARTICLE(S) OF THE CSA

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

u) where applicable, rules concerning any peer assessment mechanism established by the scheme for the authorities or bodies issuing European cybersecurity certificates for assurance level 'high' pursuant to Article 56(6). Such mechanism shall be without prejudice to the peer review provided for in Article 59.

The EUCC scheme requires that each authority or body issuing certificates at the assurance level 'high' undergo a peer assessment at periodic intervals.

While every authority or body issuing certificates (further designated under the term certification bodies, or CBs) for assurance level 'high' pursuant to Article 56.6 of the CSA, including associated testing laboratories (ITSEFs), shall operate under its own responsibility, a peer assessment shall be established to:

- assess that they work in an harmonised way and produce the same quality of certificates;
- allow the reuse of certificates for composite product certification, as offered by Chapter 2, PURPOSE OF THE SCHEME;
- identify any potential strength that result out of their daily work and that may benefit to others;
- identify any potential weakness that result out of their daily work and that shall to be considered for improvement by the peer assessed CB;
- find a harmonised way to handle vulnerabilities disclosure and handling and exchange best practices regarding the handling of complaints.

Note: The peer assessment is not intended to interfere with or make judgement to the activities performed by the NCCA, as this is the subject of the peer review process as required by Article 59 of CSA. Nor shall it interfere with or make judgement to the activities performed by the National Accreditation Body (NAB).

In order to allow timely feedback with respect to questions of the national aspects of the scheme that are handled by the NCCA, a representative of the NCCA of the assessed CB shall participate to the peer assessment.

The peer assessment of each CB issuing certificates of assurance level 'high' shall take place on a regular basis, with a periodic interval that shall not exceed five (5) years.

The ECCG[31] shall establish and maintain a planning of peer assessments ensuring that this periodicity is respected, and take into consideration the level of priority that may be given to the peer assessment of a CB issuing certificates at the assurance level 'high' in case of alleged non-compliance of this CB, and in case of CBs with recent activity engaged in certifications for the first time or after a long lasting break (more than two years) .

In the case of Article 56.6.(a) of the CSA, both the conformity assessment body issuing the certificates and the NCCA proceeding to the prior approval for each individual certificate shall be subject to the peer assessment. This shall include the procedure established by of the NCCA for prior approval for each individual certificate.

In the case of Article 56.6.(b) of the CSA, both the CAB issuing the certificates and the NCCA shall be subject to the peer assessment. This shall include the general delegation requirements defined by the NCCA.

Peer assessments shall follow the procedure established in Annex 12. Unless duly justified, peer assessments shall be performed on site for the peer assessed CB and, where applicable, for a selected set of ITSEFs.

Where certification above AVA_VAN.3 for ICT products, which are not covered by a Technical Domain, has been established according to specific Protection Profiles certified under this scheme for this purpose, ICT products certified

[31] The ECCG may establish a dedicated subgroup to handle peer assessments, based on the organisation to be installed for the maintenance of the EUCC scheme (see Chapter 25, RECOMMENDATIONS FROM THE AHWG).

according to these Protection Profiles shall be considered with high priority for selection under the peer assessment mechanism.

The peer assessment team may decide to reuse results of previous peer assessments of the assessed authority or body covering part of the scope, under the following conditions:

- such results shall be not older than five (5) years;
- where previous peer assessments of the peer assessed CB were performed under a different scheme, these shall be provided with the description of the peer assessment procedures in place for that different scheme;
- the peer assessment report shall clearly indicate which parts were reused without further assessment, and which parts were reused with additional assessment;
- where the peer assessment covers a technical domain, the reuse shall not allow to avoid a visit to the peer assessed CB and related ITSEFs.

The peer assessment team shall report their findings to the ECCG in a peer assessment report, with an indication of the severity of any shortcomings. The peer assessment report shall include where necessary guidelines or recommendations on actions or measures to be taken by the peer assessed CB, as well as the measures proposed by the peer assessed CB to handle the findings.

When establishing measures to handle the findings, the peer assessed CB may ask for the support of the peer assessment team. These measures shall be transmitted to the ECCG, indicating how they intend to correct the findings, within the peer assessment report. Where necessary, the ECCG may inform the relevant:

- NCCA of the peer assessed CB for its consideration of the potential impact of the remaining findings on the certificates issued by the peer assessed CB, or any authorisation or notification related to the peer assessed CB and associated ITSEFs;
- National Accreditation Body (NAB) of the peer assessed CB for its consideration of the potential impact of the remaining findings on the accreditation of the peer assessed CB and associated ITSEFs;

and may ask for their conclusions.

The peer assessed CB and related NCCA shall have the opportunity to address with the ECCG any shortcomings and recommendations identified in the report, before the results of the peer assessment are published by ENISA. Also, the NAB shall have the opportunity to address any shortcomings and recommendations in case any have been brought up to the NAB before the results are published.

ENISA may participate in the peer assessments.

CBs shall inform applicants to certification at the assurance level ‘high’ of the CSA that their certification projects may be subject to the peer assessment installed by this scheme.

BACKGROUND INFORMATION

Peer review of NCCA is introduced by Article 59 of the CSA. It shall in particular assess:

(d) the procedures for monitoring, authorising and supervising the activities of the conformity assessment bodies;

(e) where applicable, whether the staff of authorities or bodies that issue certificates for assurance level ‘high’ pursuant to Article 56(6) have the appropriate expertise.

In addition, a peer assessment can be defined for each scheme, with scheme specific objectives defined here for the EUCC scheme in the first part of this Chapter, and requirements.

According to both the CCRA and SOG-IS MRA peer assessment is required for the CBs at a periodic cycle. Such assessments may include the testing laboratory (ITSEF) linked to the CB: the goal is there to assess the ITSEF’s technical competencies related to a Technical Domain.

This approach guarantees the high quality of evaluation activities as required for a ‘high’ level of security assurance and the harmonisation of the evaluation methods between different CAB, therefore allowing more objective results and to proceed to composite product certifications within different CAB.

It is essential that a planning is established for such activities, including reassessments, and necessary priorities associated to newcomers to certification, or those facing issues with certification. The focus in the peer assessments on certificates that would be issued above AVA_VAN.3 without technical domains and with the new possibility to establish specific PP for that purpose has also been introduced, as a way to offer an *a posteriori* control that will be beneficial for the recognition of these certificates.

The procedure in Annex makes benefit from the existing SOG-IS procedures, and takes into consideration the possibility to reuse results from other peer assessment mechanisms.

It is considered of importance that where applicable, the assessed body or authority presents the effective measures to adapt their practices and expertise accordingly to the ECCG, in order to reensure other participants to the scheme of the quality of the certificate it issues.

In cases where the quality of the certificates is considered by the ECCG not in line with the requirements of this scheme, the ECCG may inform and consult the NCCA and the National Accreditation Body of the assessed body or authority for their conclusions on the impacts on its authorisation and accreditation.

23. SUPPLEMENTARY CYBERSECURITY INFORMATION - ARTICLE 55

REFERENCE ARTICLE(S) OF THE CSA

Article 54 1. *A European cybersecurity certification scheme shall include at least the following elements:*

v) format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updating the supplementary cybersecurity information in accordance with Article 55.

Article 55 .1. *The manufacturer or provider of certified ICT products, ICT services or ICT processes or of ICT products, ICT services and ICT processes for which an EU statement of conformity has been issued shall make publicly available the following supplementary cybersecurity information*:

(a) guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ICT products or ICT services;

(b) the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity related updates;

(c) contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers;

(d) a reference to online repositories listing publicly disclosed vulnerabilities related to the ICT product, ICT service or ICT process and to any relevant cybersecurity advisories.

Article 55 .2. *The information referred to in paragraph 1 shall be available in electronic form and shall remain available and be updated as necessary at least until the expiry of the corresponding European cybersecurity certificate or EU statement of conformity.*

Certificates will provide a link to Supplementary cybersecurity information.

Such information may be required for certification activities.

All Supplementary cybersecurity information declared necessary for certification or other activities under this scheme shall be provided by manufacturers or providers to the relevant party under the conditions established by the relevant Chapters.

In particular, in accordance with the requirements of Chapter 17, CONTENT AND FORMAT OF CERTIFICATES, a link to the website and relevant pages where that information is made available shall be provided to be integrated into the certificate. Once all requirements for certification have been fulfilled, the issuing body shall request from the manufacturer or provider to provide the URL (link) so that this can be processed before the certificate can be uploaded to the ENISA Website for certification.

Manufacturers or providers of ICT products shall make Supplementary cybersecurity information in accordance with Article 55 publicly available on their websites.

The information shall be available in electronic form and in English language and shall remain available at least until the expiration of the corresponding European cybersecurity certificate. It shall be updated in accordance with the requirements of Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES.

In particular, guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ICT products, as defined by Article 55.1.(a), shall be at any time coherent with the guidance and recommendations that have been assessed during the evaluation, or updated. When different from the latter, these may be submitted for review to the evaluator of the ICT product, as to allow assessing the expected coherence.

BACKGROUND INFORMATION

In addition to the public availability of the information, as requested by Article 55, the need for having access to all or part of it during certification may be requested, such as to test that the information complies with the requirements of the scheme. This way the procedure also sees to it that the manufacturer should have the URL up and running before the certificate is issued. This specific need to review part of Supplementary cybersecurity information during the certification phase shall however only occur where the relevant Chapters of this scheme establish a requirement to do so.

For an easy and harmonised access of users of certificates to the webpages where the information will be accessible on the Websites of manufacturers or providers, the associated link will have to be provided in the certificate.

The conditions to deliver the Supplementary cybersecurity information should be part of a more detailed disclosure policy that ENISA will establish in accordance with the requirements of Chapter 20, DISCLOSURE POLICY FOR CERTIFICATES.

24. ADDITIONAL ELEMENTS OF THE SCHEME

24.1 CERTIFICATION OF PROTECTION PROFILES

REFERENCE ARTICLE(S) OF THE CSA

Article 54 1. *A European cybersecurity certification scheme shall include* *<u>at least</u>* *the following elements:*

a) the subject matter and scope of the certification scheme, including the type or categories of ICT products, ICT services and ICT processes covered.

The cybersecurity evaluation and certification of Protection Profiles (PP), a formal document defined according to the CC expressing an implementation-independent set of security requirements for a category of ICT products that meet specific consumer needs, shall be an additional element to the EUCC scheme.

The certification of a Protection Profile shall demonstrate that the PP is complete, consistent, and technically sound and suitable for use as a template on which to build another PP or a Security Target.

In addition to the certification of ICT products, the scheme shall as well cover the certification of Protection Profiles.

It shall be based on the same conditions of this scheme that apply for the certification of an ICT product that would ultimately be certified in accordance with the Protection Profile, with the following exceptions:

- its evaluation shall be limited to the subset of activities associated to the APE criteria as listed in the CC Part 3;
- the Protection Profile may be, as an ICT product, subject to maintenance for updates or corrections, and shall not necessitate the application of the monitoring activities described under Chapter 11, RULES FOR MONITORING COMPLIANCE nor of those described under Chapter 14, RULES RELATED TO HANDLING VULNERABILITIES;
- the certificate of a Protection Profile shall be a subset of the certificate of an ICT product;
- Supplementary cybersecurity information as defined by Article 55 shall not be necessary.

The certificate of a Protection Profile shall indicate the Assurance level targeted for ICT products that will comply with this Protection Profile, in accordance with the mapping detailed in Chapter 4, ASSURANCE LEVELS and shall include the following elements:

- a unique identifier established by the issuer of the certificate;
- information related to the certified ICT Protection Profile and its developer:
  - name of the ICT Protection Profile;
  - type of the ICT Protection Profile;
  - version for the ICT Protection Profile;
  - name and contact information of the developer;
- information related to the evaluation and certification of the ICT Protection Profile:
  - name and contact information of the CB that issued the certificate;
  - name of the ITSEF which performed the evaluation, when different from the certification body;
  - name of the responsible NCCA;
  - reference to this scheme;
  - reference to the certification report associated with the certificate;
  - assurance level from the CSA reached (either 'substantial' or 'high');
  - identification of the used assurance components from the CC, including the AVA_VAN level covered;
  - where applicable, reference to Protection Profile(s) to which the ICT Protection Profile complies;
  - date of issuance.

The certification report associated to the certificate shall include the relevant sections of Annex 13, related to the previous list.

BACKGROUND INFORMATION

The Common Criteria methodology provides the opportunity to define in the form of Protection profiles (PP) an implementation-independent set of security requirements for categories of ICT products that meet specific consumer needs. PPs are widely used by consumer groups and communities of interest, and as such may become standards while being referenced into EU regulation.

Security of information used for and created by certification shall be ensured.

Such PPs can be evaluated and certified as well, using the same methodology.

According to the CC Part 1: PP evaluation is optional. Evaluation is performed by applying the APE criteria to them as listed in CC Part 3. The goal of such an evaluation is to demonstrate that the PP is complete, consistent, and technically sound and suitable for use as a template on which to build another PP or an ST. Basing a PP/ST on an evaluated PP has two (2) advantages:

- there is much less risk that there are errors, ambiguities or gaps in the PP;
- evaluation of the new PP/ST may often re-use evaluation results of the evaluated PP, resulting in less effort for evaluating the new PP/ST.

PPs are not ICT products and shall not be subject to the same rules of maintenance. As such, there certificates do no not indicate any validity period, as it is more of a matter of the stakeholders communities that developed these PPs to decide on when the PPs should terminate to be considered or applicable for ICT products.

24.2 SECURITY OF INFORMATION

REFERENCE ARTICLE(S) OF THE CSA

Annex item 16: *The conformity assessment body and its staff, its committees, its subsidiaries, its subcontractors, and any associated body or the staff of external bodies of a conformity assessment body shall maintain confidentiality and observe professional secrecy with regard to all information obtained in carrying out their conformity assessment tasks under this Regulation or pursuant to any provision of national law giving effect to this Regulation, except where disclosure is required by Union or Member State law to which such persons are subject, and except in relation to the competent authorities of the Member States in which its activities are carried out. Intellectual property rights shall be protected. The conformity assessment body shall have documented procedures in place in respect of the requirements of this point*.

Unless otherwise provided for in this scheme and without prejudice to existing national provisions and practices in the Member States on confidentiality, all parties involved in the application of this Scheme shall respect the confidentiality of information and data obtained in carrying out their tasks in order to protect the following:

a) personal data, in accordance with GDPR[32];
b) commercially confidential information and trade secrets of a natural or legal person, including intellectual property rights, during the certification lifecycle of the product and up to the end of the indicated retention time for all certification information, unless disclosure is necessary in the public interest, or subject to court orders;
c) information necessary for the effective implementation of this scheme, in particular for the purpose of peer reviews, peer assessments or audits, effective collaboration between the involved authorities and bodies, the handling of publicly unknown and subsequently detected vulnerabilities in the process of, or after certification, and the handling of complaints.

Without prejudice to previous paragraph, information exchanged on a confidential basis between competent authorities and between competent authorities and the Commission shall not be disclosed to the public without the prior agreement of the originating authority.

[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

All information received from the CABs (CBs, and associated ITSEFs) or the manufacturers or providers shall only be used for the purpose of the certification and deemed confidential by the NCCAs - unless a different agreement is reached between the parties or unless an information flow is required by a specific regulation of the scheme.

ENISA may provide in cooperation with the ECCG guidance on how to ensure the security of information based on the workflows associated with the activities described in the EUCC scheme.

BACKGROUND INFORMATION

Security of information is key in cybersecurity related activities. All cybersecurity certification related activities fall into the latter.

Information provided by the applicant to the CAB for certification might be sensitive, especially as, the higher the evaluation level, the deeper the evaluator shall go into the analysis of the ICT product and related life-cycle, based on information details that may comprise commercially confidential information and trade secrets, including intellectual property rights.

Information developed by cybersecurity certification activities, such as Evaluation Technical Reports and associated to vulnerabilities assessment, handling and release, will also contain information sensitive parts that, when poorly protected, may obviously endanger the users of associated products, even when these products are certified.

Therefore, the obligations of the different actors of the scheme to ensure the security of information shall be established and take into consideration the requirements for manufacturers and developers to comply with Article 55 of the CSA, and the necessary respect of Freedom of Information policies and legal frameworks, Access to Information Acts, and/or any other similar national, European and international policies and regulations by any individuals or entities.

25. RECOMMENDATIONS FROM THE AHWG

25.1 RECOMMENDATIONS FOR THE ADOPTION OF THE EUCC SCHEME

REFERENCE ARTICLE(S) OF THE CSA

Article 57 1. *Without prejudice to paragraph 3 of this Article, national cybersecurity certification schemes, and the related procedures for the ICT products, ICT services and ICT processes that are covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant to Article 49(7). National cybersecurity certification schemes and the related procedures for the ICT products, ICT services and ICT processes that are not covered by a European cybersecurity certification scheme shall continue to exist.*

The AHWG recommends the following for the adoption of the EUCC scheme, considering the necessary transition from the SOG-IS MRA.

Based on its experience, the AHWG recommends a transition period of two (2) years to adopt the new rules while introducing no market disruption. Any shorter period should be accompanied with temporary derogations to the EUCC rules.

BACKGROUND INFORMATION

The transition period is here considered as the period between the date of adoption of the implementing act adopted pursuant to Article 49(7), and the date established into this implementing act when national schemes shall cease to product effect.

Based on the discussions with the EC, the scenario of a “big bang” has been considered as the most probable one, being it consists of the following:

- all existing schemes cease at the same date;
- there is zero parallel emission of EUCC and SOG-IS MRA certificates for the same ICT products during the transition period.

RECOMMENDATIONS

First, the transition period should technically allow the ICT products cybersecurity certification ecosystem using the SOG-IS MRA to adopt the new rules installed for the EUCC scheme, in particular:

- existing and new CBs to be accredited to ISO/IEC 17065;
- existing and new ITSEFs to be accredited to ISO/IEC 17025;
- new private CABs to be installed for the ‘substantial’ level;
- CBs to be authorised with their ITSEF for the level ‘high’;
- manufacturers or providers of ICT products to get familiar with and adopt maintenance mandatory requirements, as well as vulnerability handling and release rules;
- NCCA and CB to put monitoring activities in place;
- NCCA to put market surveillance in place;
- a maintenance organisation of the scheme to be in place to further develop the scheme and to support any interpretation and harmonisation question related to the adoption of the new scheme.

Then, any market disruption of the certification activities should be avoided. In particular, the transition period should allow for:

- termination of current certification projects under the existing schemes, or their easy conversion into EUCC projects;
- smooth transfer of certificates that require maintenance in the long run, therefore under for the EUCC scheme, or reuse for composite evaluations and certifications under the EUCC scheme.

Lastly, it should allow for the installation of the conditions to establish a CCRA-type of MRA with third countries, as well as a label to promote EU certificates.

The candidate scheme has introduced some possible reuse conditions as to ease the transition (e.g., reuse of certification activities or reuse of peer assessment results).

However, this could not occur to all requirements associated to the EUCC scheme, in particular, the accreditation of all CBs and ITSEFs that wish to continue activities under the EUCC. This is considered both an important requirement and based on the experience of the AHWG members a time demanding activity (which may take more than a year - especially as not all national existing interpretations of the related standards have been harmonised so far). Market surveillance activities are also new activities introduced by the CSA.

Therefore, the AHWG would recommend a transition period of two (2) years as a technically acceptable one.

When shortened, this should be accompanied with potential temporary derogations to the rules adopted within the EUCC scheme, especially as to reduce the delays of the technical difficult transition steps as mentioned before. ENISA could be tasked to support the ECCG for the development and proposal of an analysis of such possible derogations.

In any case, ENISA should also support the development of transitions recommendations for a smooth transition of certificates and certification activities.

25.2 RECOMMENDATIONS FOR THE MAINTENANCE OF THE EUCC SCHEME

REFERENCE ARTICLE(S) OF THE CSA

Article 62.4 *The ECCG shall have the following tasks:*

e) to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes.

The AHWG recommends the following for the maintenance of the EUCC scheme, considering the existing groups supporting the SOG-IS MRA.

The ECCG should mandate groups of experts involving NCCA, CAB and associated testing facilities, and manufacturers or providers of ICT products to:

- improve evaluation methods and testing;
- support the development of new Technical Domains;
- support the development of specific Protection Profiles that would permit, in accordance with the conditions defined in Chapter 4, ASSURANCE LEVELS, the certification above AVA_VAN.3 for ICT products that are not covered by a Technical Domain;
- provide written guidance on Protection Profiles harmonization

The expert groups should focus on methodology harmonization of testing, analysis of new attacks and applicability to ICT products (rating, updating of test methodology), and propose new or revised supporting documents.

This is especially relevant for the assurance level ‘high’ of the CSA.

They should be organised in order to cover any generic and specific domain, and the ECCG should consider the existing terms of reference of the existing structure supporting the current SOG-IS MRA[33].

Expert groups could also be used as consultants to ascertain for the benefit of the ECCG whether certain attacks have cross contamination amongst certificates within a specific domain or even across domains.

ENISA should publish the list of mandated expert groups and their associated mandates.

Groups of experts involving NCCA, CAB and their testing facilities, and manufactures or providers of ICT products should be considered as to further develop harmonised requirements for the scheme.

[33] https://www.sogis.eu/uk/detail_operation_en.html

26. REFERENCES

CSA *(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.

SOG-IS MRA
Mutual Recognition Agreement of Information Technology Security Evaluation Certificates VERSION 3.0, MANAGEMENT COMMITTEE, January 2010.

CCRA
ARRANGEMENT on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2, 2014.

REFERENCED STANDARDS

Table 6: Standards references

Reference	Title
ISO/IEC 15408	Information technology - Security techniques - Evaluation criteria for IT security
ISO/IEC 18045	Information technology - Security techniques - Methodology for IT security evaluation
ISO/IEC 17000	Conformity assessment - Vocabulary and general principles
ISO/IEC 17065	Conformity assessment - Requirements for bodies certifying products, processes and services
ISO/IEC 17025	Testing and calibration laboratories
ISO/IEC 19896-3	IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators
ISO/IEC WD TS 23532-1	IT Security Techniques — Requirements for the competence of IT security testing and evaluation laboratories — Part 1: Testing and evaluation for ISO/IEC 15408
ISO/IEC 27001	Information technology - Security techniques - Information security management systems – Requirements
ISO/IEC 27002	Information technology - Security techniques - Code of practice for information security management controls
ISO/IEC 27005	Information technology - Security techniques - Information security risk management
ISO/IEC 29147	Information technology - Security techniques - Vulnerability disclosure
ISO/IEC 30111	Information technology - Security techniques - Vulnerability handling processes
ISO/IEC 7816-4	Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange

27. ANNEX 1: ASSURANCE PACKAGE DECLARATION IN A CERTIFICATE

PURPOSE

Chapter 17, CONTENT AND FORMAT OF CERTIFICATES defines the minimum information to be included in all certificates for ICT products issued under the EUCC Scheme, and indicates the possibility to declare augmented assurance packages, as authorised by the CC.

The purpose of this annex is to clarify the required information on the assurance level or package in the certificate to avoid misuse and misunderstanding by users.

PARTICULAR STATUS

None.

CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE

Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS.
Chapter 17, CONTENT AND FORMAT OF CERTIFICATES

The assurance package confirmed in a certificate shall distinguish between CC Part 3 Evaluation Assurance Level (EAL) conformant and CC Part 3 EAL augmented.

An augmentation shall be designated by listing the augmented components abbreviations.

An augmentation shall be outlined in detail in the certification report. The certificate itself may include additional information of the augmented component, e.g. the full name of the component like "AVA_VAN.5 Advanced methodical vulnerability analysis".

Examples:

- CC Part 3 conformant EAL4 augmented by ALC_FLR.2 and AVA_VAN.5;
- or CC Part 3 conformant EAL4 augmented by ALC_FLR.2 - Flaw reporting procedures and AVA_VAN.5 - Advanced methodical vulnerability analysis.

The "+" as an abbreviation for an EAL augmentation shall not be used.

In case a certificate does not confirm any EAL, the certificate shall at least indicate: "Specific assurance package" or in case of a claim towards a Protection Profile without an EAL: "Assurance package conform to PP".

28. ANNEX 2: MINIMUM SITE SECURITY REQUIREMENTS

PURPOSE

This annex defines a set of minimum requirements that a developer shall meet and that an evaluator can verify during any type of evaluation under the EUCC scheme in order to ensure compliance with ALC_DVS.1 and ALC_DVS.2 in a manner consistent with today's standard practices for evaluations requiring attack potential associated with AVA_VAN.5.

PARTICULAR STATUS

These minimum requirements can be considered as guidance for other evaluation levels..

CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE

Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS.

1 INTRODUCTION

1.1 Objective

The CEM describes in ALC_DVS family what the evaluator has to examine with regard to developer security but does not define the minimum site security requirements.

The purpose of this annex is to define a set of minimum requirements that a developer shall meet and that an evaluator is able to verify during any type of evaluation under the EUCC scheme in order to ensure compliance with ALC_DVS.1 and ALC_DVS.2 in a manner consistent with today’s standard practices for evaluations requiring an attack potential associated with AVA_VAN.5.

The requirements set in this annex are “minimum” in the sense that:

-all developers have to implement the controls and related security measures defined in this annex;
-additional requirements could apply to facilitate the ST, or to meet the protection needs of the TOE.

1.2 Clarification on other deliverables related to the scope of site audits

From EAL3, ALC_DVS.1 is required and ALC_DVS.2 is expected for EAL6. Due to the reference to high attack potential as used for AVA_VAN.5, a common practice is to consider ALC_DVS.2 as a standard augmentation to EAL4.

ALC_CMS.3 and ALC_CMS.4 have dependency to ALC_DVS.1 and ALC_CMS.5 has dependency to ALC_DVS.2. Other ALC families as ALC_CMS, ALC_DEL and ALC_TAT requires site visit to confirm that developer practices are consistent with documentation evidences

Therefore, some work units of ALC_CMC, ALC_CMS, ALC_DEL and ALC_TAT described in the CEM require that documentary evidence should be supplemented by visiting the development environment in order to check the evidence that the procedures are being applied.

This annex covers the controls that shall be considered for the development environment to have the appropriate level of protection to maintain confidentiality and integrity of the TOE corresponding to the overall attack potential as used for AVA_VAN.5 and claimed for the TOE. The specified objectives are consistent and mutually supportive.

1.3 Structure of the annex

Section 9 consists of one or more security controls. All controls have to be considered by the developer but may be omitted with the necessary justification, where not applicable. The Asset Management section defines the assets to be protected, the necessary policies, and their content in order to be compliant with the CEM, and following sections detail the security controls with objectives and describes the security measures that are necessary to protect the assets related to the TOE.

Each control is defined into 4 parts:

- Objective - defines the mandatory target of the control, i.e. what shall be achieved by the respective security measures. As long as a control is applicable the objectives cannot be omitted;
- Policies - defines the policies mandatory to facilitate the objective;
- Security Measures - describes the expected security measures that are necessary to protect the assets related to the TOE. Security measures shall be modified, replaced, or omitted only with justification, providing clear evidence that the required level of security is achieved;
- Examples - illustrate requirements with typical set-up or implementation, where appropriate. These examples are for explanation purpose and do not have to be systematically implemented as is.

The controls and control objectives described in this document are not exhaustive; additional control objectives and controls may also be selected, where necessary.

1.4 Application

The current annex shall apply for the evaluation of ICT products related to the Technical Domain of smart cards and similar devices, including related software development. Related software comprises software necessary to operate the smart cards and similar devices (firmware, operating system), software which contributes to the security of smart cards and similar devices, and software running on the smart cards and similar devices.

The requirements are specifically aimed at an evaluation where the attacker has a high attack potential (AVA_VAN.5).

This annex may also be considered as guidance for security evaluations of sites associated to other ICT products, whenever ALC_DVS appears in the assurance criteria to be met. In all cases, the attack potential of the threat agent shall be considered in accordance with the selected AVA_VAN level when determining whether the deployed measures are sufficient.

For the Technical Domain related to hardware boxes with security measures, not all manufacturing sites which produce electronic components (e.g. ICs, transistors, resistors, memory chips) composing the TOE will need to be checked. However, the security relevant sites shall be visited: this includes the sites related to a) the TOE development, b) the final assembly where the integrity and authenticity (if applicable) of all incoming, security relevant parts of the TOE is verified, c) the initial key loading and d) other sites if explicitly required by a Protection Profile (PP) to which the ST refers.

This annex is based on CEM paragraphs 1102ff. and CEM Annex A.4.3.2. The requirements are structured according to ISO/IEC 27001.

Note: although based on ISO/IEC 27001, further detailed specification of objectives and security measures are considered as an extension of controls defined in this standard. This is why applying only the standard is not considered as sufficient, and why an information security management system certified according to ISO/IEC 27001 is neither necessary nor sufficient to satisfy the requirements of the EUCC scheme defined in this annex.

The requirements in this annex apply to environments used for the development (all steps of the life cycle until delivery) of the TOE and shall be interpreted from a TOE perspective in terms of confidentiality, integrity or authenticity.

The requirements set out in this annex are generic and are intended to be applicable to all organizations, regardless of type, size, and nature. No particular requirements from a PP have been included.

1.5 Developer

In order to fulfil the CC requirements for ALC_DVS, the developer shall achieve all applicable objectives set in this document. Therefore, appropriate measures, typically as described in the sub-sections related to security measures, shall be implemented in a meaningful and concerted way.

The developer has to consider all the controls specified in this document in order to pass site security evaluation. Any exclusion of controls needs to be justified and shown not to affect the developer’s ability, and/or responsibility, to provide a level of security that meets the security needs derived from the ST and the objectives defined in this document.

If the developer implements a different security setup, e.g. modified, replaced, or omitted security measures, he/she has to ensure and to demonstrate that the objectives are fulfilled and the required level of security is achieved. Developer shall provide justification to the evaluator.

The developer can refer to this document in order to support justification that the measures maintain confidentiality and integrity.

1.6 ITSEF

Consistently with §13.5 of CEM, the objective is to determine whether the developer's security controls on the development environment are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure that secure operation of the TOE is not compromised.

ALC_DVS targets all the sites at which TOE development occurs and that are identified in the development security documentation. This annex must be used for the assessment of each of these sites.

ALC_DVS.1.1 and ALC_DVS.2.1 specify that the evaluator shall examine the development security documentation to determine that it details all security measures used in the development environment that are necessary to protect the confidentiality and integrity of the TOE design and implementation.

In order to determine the sufficiency of the security measures employed, the ITSEF shall examine:

- the development confidentiality and integrity policies and assumptions of the ST;
- the justification (e.g. risk assessment) for any exclusion or incomplete implementation of controls, and;
- the correct and concerted implementation of the measures required in the controls.

If the ST identifies security objective(s) for the development environment that call for specific requirements for the policies, the evaluator shall take it(them) into account for the assessment.

ALC_DVS.2.2 specifies that the evaluator shall examine the development security documentation to determine that an appropriate justification is given why the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

The evaluator shall examine the correct and concerted implementation of the measures required in the controls. If the developer implements the controls incompletely or with different security measures than the expected ones the justification provided by the developer should include a demonstration that the required level of security is achieved.

The evaluator shall examine this demonstration and determine whether or not the objectives defined in chapter 9 of this document are achieved.

The evaluator shall determine that the justification takes into consideration the ST for any information that may require additional requirements for the development environment security.

The evaluator shall determine that the justification covers all aspects of development and production on all the different sites with all roles involved up to delivery of the TOE and that the application of this document to these different stages and sites is done correctly and consistently.

The requirements defined in this document should be used by the evaluator to create a checklist to prepare the site visit and the examination of evidence that are required by ALC_DVS.1.3 and ALC_DVS.2.4.

2 NORMATIVE REFERENCES

Following documents are indispensable for the application of this annex. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- Common Criteria for Information Technology Security Evaluation, Part 1-3, April 2017, Version 3.1 release 5;
- Common Methodology for Information Technology Security Evaluation, Evaluation methodology, April 2017, Version 3.1 release 5;
- ISO/IEC 27002, Information technology - Security techniques - Code of practice for information security management controls.

The following standards may be beneficial in implementing the respective processes.

- ISO/IEC 27001, Information technology - Security techniques - Information security management systems – Requirements;
- ISO/IEC 27005, Information technology - Security techniques - Information security risk management.

3 TERMS AND DEFINITIONS

For the purposes of this annex, the following terms and definitions apply.

Assets: Entities that the owner of the TOE presumably places value upon.
In the context of a Development Security System, assets are information in electronic or other form, information processing facilities and referring processes (incl. access control and alarm systems), development tools and environments, any manifestation of the TOE, and customer code and data provided to produce the TOE

Availability: The property of being accessible and usable upon demand by an authorized entity.

Business operations: General term for the entirety of operations performed by the developer related to the TOE, e.g. “personalization” is part of business operations.

COBIT: Control Objectives for Information and Related Technology.

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Control: Set of measures, associated to one or more objectives, intended to respond to threats.

Data processing facilities: Premises, equipment, installation or tool used for data processing.

Developer: Entity (Site) offering services and being part of the development and production process; this encompasses all steps of the life cycle until delivery to the customer, e.g. software development, chip design, mask making, wafer production, testing, assembly etc. The developer is also responsible for supporting functions.

Development environment: Environment in which the TOE is developed; development includes the production of the TOE.

DMZ: Demilitarized Zone; in computer security, a DMZ is a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet.

DSD: Development Security Documentation.

DSS: Development Security System.

Employment: The word 'employment' is meant here to cover all of the following different situations: employment of people (temporary or longer lasting), appointment of job roles, changing of job roles, assignment of contracts, and the termination of any of these arrangements.

Facility: Any equipment, installation or tool, regardless of being software or hardware, which is part of the security management system.

FW: Firmware.

High Security Area: Area where TOE related data or material classified “critical” or “very critical” is accessible, and Security Control areas (access control and intrusion detection) where applicable.

Information security (IS): Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

Integrity: The property of safeguarding the accuracy and completeness of assets.

IS event: An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

IS incident: A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

ISMS: Information Security Management System.

ITIL: Information Technology Infrastructure Library.

Malicious code: Virus, worms, Trojans, spyware and adware based on the perceived intent of the author.

Mobile code: Software obtained from remote systems transferred across the network, e.g. Java code, activeX controls, flash animations, office macros etc.

Mobile Computing: Data processing on a mobile device, either online or offline; mobile computing uses communications technology to work in uncontrolled environments outside developer's premises

MSSR: Minimum Site Security Requirements, abbreviation for this document.

Network architecture: Framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, as well as data formats used in its operation.

Organization: Group of people and facilities with an arrangement of responsibilities, authorities and relationships.

Organizational Security Policy: Set of security rules, procedures, or guidelines for an organisation.

OS: Operating System.

Owner: The term owner identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term owner does not mean that the person has any property rights to the assets.

Partner: Any organization which has been part of the supply chain within the past two years, e.g. development company, mask house, production site, test floor, assembly line, regardless of their ownership.

Policy: Set of security rules, procedures, or guidelines for an organization; a policy may pertain to a specific operational environment.

Procedure: A specified way to perform an activity.

Process: A sequence of activities or procedures.

Reliability: The ability of either a facility or a procedure to perform a required function over time.

Remote access: Connection to a data processing system from a location off premises by means of a network connection where:
- the connection is from outside the logical security environment;
- the working location is outside the physical security environment.

Residual risk: The risk remaining after risk treatment.

Risk acceptance: Decision to accept a risk.

Risk analysis: Systematic use of information to identify sources and to estimate the risk.

Risk assessment: Overall process of risk analysis and risk evaluation.

Risk evaluation: Process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

Risk management: Coordinated activities to direct and control an organization with regard to risk.

Risk treatment: Process of selection and implementation of measures to modify risk.

SAM: Secure Access Module (or Secure Application Module).

Sensitive data: Data which needs protection in order to support confidentiality and/or integrity requirements.

Strong authentication: Authentication with at least two independent factors, e.g. possession and knowledge (badge and PIN), or possession and individual attribute (badge and biometrics).

Team member: The term “team member” encompass employees, contractors, consultants, students, and third party users involved in the secure processes or having access to protected information.

Teleworking: Working via remote access; teleworking uses communications technology to work remotely from a fixed location outside developer's premises.

Third party user; Any user who is not employee, contractor, consultant, or student, e.g. customer, ITSEF, CB.

Threat: Any circumstance or event with the potential to adversely impact organizational operations, assets (incl. TOE or its parts), or individuals via unauthorized access, destruction, disclosure, modification, and/or denial of service. Also, the potential for a threat-source to successfully exploit particular system vulnerability. The Common Criteria characterizes a threat in terms of (a) a threat agent, (b) a presumed method of attack, (c) any vulnerability that is the foundation for the attack, and (d) the system resource that is attacked.

Top Management: Highest ranking executives (with titles such as chairman/chairwoman, chief executive officer, managing director, president, executive directors, executive vice-presidents, etc.) responsible for the entire enterprise. In organizations where the developer is not the only activity “Top Management of the developers’ organization” may refer to the management of a division, business group, product line etc.

VPN: Virtual Private Network; the term secure VPN is used for VPNs without potential eavesdropping risk, e.g. by the use of IPSec or SSL encrypted tunnels or special physically secured in-house links if another security zone is crossed.

ISO terminology, such as "can", "may", "normative", "shall" and "should" used throughout the annex are defined in the ISO/IEC Directives, Part 2:

(Note that the term "should" and “informative” have an additional meaning applicable when using this standard. See the note below.)

- the word “shall” indicates measures strictly to be followed in order to conform to the annex and from which no deviation is permitted.
- the word “should” indicates that among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required. ISO/IEC 15408 series interprets “not necessarily required” to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.
- the word “may” indicates a course of action permissible within the limits of the annex.
- the word “can” is used for statements of possibility and capability, whether material, physical or causal.
- the expression “confidentiality and/or integrity” means either “confidentiality” or “integrity”, or a combination of both.
- the expression “informative” indicates measures that are not mandatory to follow in order to conform to the document.

4 DEVELOPMENT SECURITY SYSTEM AND DOCUMENTATION

4.1 Objective

As required by ALC_DVS.1.1C and ALC_DVS.2.1C, respectively, the Development Security Documentation (DSD) shall describe the physical, logical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

DSD shall identify all locations where development occurs, the development activities, and the security measures applied at each location linked to such activities and for transports between different locations.

If ALC_DVS.2 is claimed, the development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE according to the attack potential claimed in the ST (AVA_VAN.5).

4.2 Policies

The evaluation evidence for the evaluation of development security is the ST and the development security documentation (DSD). Therefore, the developer has to establish, implement, operate, monitor, maintain, review, and improve a documented development security system (DSS) within the context of the organization's overall business activities and the risks it faces.

The DSD shall document and the evaluator shall examine the development confidentiality and integrity policies that detail:

- what information relating to the TOE development needs to be kept confidential, and which members of the development staff are allowed to access such material;
- what material must be protected from unauthorised modification in order to preserve the integrity of the TOE, and which members of the development staff are allowed to modify such material.

Policies shall contain a description of developers organization, relevant roles, and the security measures implemented. According to ALC_DVS the following types of security measures shall be considered for documentation:

- Physical, e.g. access control and intrusion detection;
- Procedural, e.g. granting and revoking access rights, transfer of protected material, roles and responsibilities for security personnel;
- Personnel, e.g. check of trustworthiness;
- Other security measures, e.g. logical protection of any development machines.

4.3 Security Measures

The threats to be covered by appropriate security measures include:

- "Accidental threat": a possibility of human error or omission, unintended equipment malfunction, or natural disaster;

- "Intentional threat": a possibility of an attack by an intelligent entity (e.g. an individual hacker or a criminal organization). Examples for such attacks are theft and pilferage, intentional exchange of the TOE or its parts, and cloning.

When justification is required, this annex can be used as a basis after adaptation to the developer specific situation and environment.

The ability to demonstrate the link from the selected controls back to the results of the risk assessment and risk treatment process, and subsequently back to the DSD policy and objectives, can support both, ITSEF work packages and justification according to ALC_DVS.2.2C.

Control of documents
Documents required by the DSS should be controlled and protected. A documented procedure should be established to define the management actions needed to:

- approve documents for adequacy prior to issue;
- review and update documents as necessary and re-approve documents;
- ensure that changes and the current revision status of documents are identified;
- ensure that documents remain legible and readily identifiable;
- ensure that documents are available to those who need them, and are transferred, stored and ultimately disposed of in accordance with the procedures applicable to their classification;
- prevent the unintended use of obsolete documents;
- apply suitable identification to them if they are retained for any purpose.

Establishing and managing the DSS and DSD
According to the CEM, ALC_DVS.1-2 requires the evaluator to examine the development confidentiality and integrity policies in order to determine the sufficiency of the security measures employed.

The developer is free to structure the DSD as appropriate. It may consist of the developers ISO 27001 Information Security Management System, be structured according to this annex, or be structured in any way suitable for the developer.

In order to support this ITSEF work package, the developer should:

- define a Security Policy that includes a framework for setting objectives and establishes an overall sense of direction and principles for action with regard to the integrity and confidentiality needs of the TOE;
- define the risk assessment approach of the organization including a risk assessment methodology that is suited to the DSS, the identified security, and legal and regulatory needs to protect the TOE;

Note: Risk assessment is intended to identify, analyse and evaluate risks, identify, evaluate, and select control objectives and controls for the treatment of risks, and produce comparable and reproducible results.

- formulate a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing security risks;
- implement the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities;
- describe all selected control objectives and controls and their implementation, including the necessary processes and operation procedures.

The DSD should include:

- documented statements of the DSS policy and objectives;
- the scope of the DSS as far as the TOE is concerned;
- procedures and controls in support of the DSS;
- documented procedures needed by the organization to ensure the effective planning, operation and control of its developer security processes.

Monitor and review the DSS
The developer should:

- execute monitoring and reviewing procedures and other controls to:
  - promptly detect errors in the results of processing;
  - promptly identify attempted and successful security breaches and incidents;
  - enable management to determine whether the security activities delegated to people or implemented by technology are performing as expected;
  - help detect security events and thereby prevent security incidents by the use of indicators;
  - determine if the actions taken to resolve a breach of security were effective;
- undertake regular reviews of the effectiveness of the DSS taking into account results of security audits, incidents, results from effectiveness measurements, and suggestions and feedback from all interested parties;
- review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks;
- conduct internal DSS audits at planned intervals defined in DSD;
- update security plans to take into account the findings of monitoring and reviewing activities.

Maintain and update the DSD
In order to ensure the DSD is up to date the developer regularly:

- should implement the identified improvements of the DSS in the DSD;
- should take appropriate corrective and preventive actions in accordance with the section dedicated to DSS improvement;
- may apply the lessons learnt from the security experiences of other organizations and those of the organization itself;
- should communicate the actions and improvements to all interested parties with a level of detail appropriate to the circumstances and, as relevant, agree on how to proceed.

Control of records
Records should be established and maintained to provide evidence of conformity to requirements, including the effective operation of the DSS. They should be appropriately protected and controlled. Records should remain legible, readily identifiable and retrievable. The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records should be documented and implemented.

Records should be kept of the operation of the processes and of all occurrences of significant security incidents related to the DSS.

4.4 Examples

It is common practise to define the scope and boundaries of the DSS with respect to the characteristics of the organization, its location, assets and technology, and including details of and justification for any exclusion from the scope.

Rules and regulations regarding document hierarchy, document structure, release procedures etc. are often defined in the Quality Management System according to ISO 9000 series of standards. Usually, the QMS also defines the approach to preventive and corrective measures, audit schemes, and management review.

An Information Security Management System according to ISO 27000 series of standards defines all necessary measure to preserve the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed. ISMS documentation refers to developer’s ITIL and/or COBIT framework.

Where the EUCC relevant activities are part of a bigger organization, special security measures are described in additional documentation. That may be additional chapters in the above mentioned documents, a dedicated document containing special regulations and referring to the above mentioned documents for all common regulations, or a dedicated DSD.

5 MANAGEMENT RESPONSIBILITY

5.1 Objective

The developer shall have well defined, documented, and assigned roles and responsibilities for all activities which may have an impact on confidentiality and integrity of the TOE.

All resources necessary to maintain confidentiality and integrity of the TOE shall be identified and available.

All physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE shall be effective.

5.2 Policies

The overall Security Policy shall define developer's approach to security and the area of applicability. It shall establish an overall sense of direction and principles for action with regard to confidentiality and integrity needs of the TOE.

5.3 Security Measures

Top Management should define developer's legal and organizational structure and is responsible for confidentiality and integrity of the TOE.

Management commitment
Top Management should support establishment, implementation, operation, monitoring, review, maintenance and improvement of the DSS, at least by assigning one or more people to the role of Security Manager and providing necessary resources.

Security Manager
The Security Manager(s) should be responsible for overall security within the developers' area of responsibility throughout the whole development life cycle of the TOE, including any subcontractors that may be used. In this function, the Security Manager should report to the Top Management of the developers' organization. The objectives and task of the Security Manager include but are not limited to the requirements described in this Section.

Resource management
The organization should determine and provide the resources needed to satisfy the requirements set in this annex. Determination should be updated regularly or after significant change of threats or environment.

Developer shall be responsible for all resources used regardless ownership.

All roles and responsibilities involved with developers' activities should be well defined and documented, e.g. work-flows, role descriptions, org-chart.

All personnel, including members of external parties, shall be competent to perform the assigned tasks.

Where appropriate, organizational measures should ensure segregation of duties between development, production, testing, quality assurance, and security.

Confidentiality agreements
Requirements for confidentiality or non-disclosure agreements reflecting the developer's needs for the protection of information, data, and material should be identified and regularly reviewed.

The necessary agreements should be concluded.

6 INTERNAL DSS AUDITS

6.1 Objective

Internal audits shall ensure that security measures are implemented in a meaningful and concerted way, and that security measures effectively support the intended purpose.

6.2 Policies

The responsibilities and requirements for planning and conducting audits, for reporting results, and maintaining records shall be defined in a documented procedure.

6.3 Security Measures

The organization should conduct internal DSS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its DSS:

- conform to the requirements of this Requirement Document;
- conform to the identified security needs of the TOE;
- are effectively implemented and maintained;
- are performing as expected.

An audit program should be planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audit criteria, scope, frequency and methods should be defined. The selection of auditors and conduct of audits should ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work.

The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities should include the verification of the actions taken and the reporting of verification results.

7 MANAGEMENT REVIEW OF THE DSS (INFORMATIVE)

7.1 Objective

Management should ensure that developer has well defined, documented, and assigned roles and responsibilities for all activities which may have an impact on confidentiality and integrity of the TOE.

All physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE should be effective.

7.2 Policies

The management review process should be documented.

7.3 Security Measures

Management should review the organization's DSS at planned intervals, or when significant changes to the security implementation occur, in order to ensure its continuing suitability, adequacy and effectiveness. This review may include assessing opportunities for improvement and the need for changes to the DSS. The results of the reviews should be clearly documented and records should be maintained.

Review input
The input to a management review should include:

- results of DSS audits and reviews;
- feedback from interested parties, particularly Evaluation and Certification Bodies;
- status of preventive and corrective actions;
- vulnerabilities or threats not adequately addressed in the previous risk assessment;
- follow-up actions from previous management reviews;
- any changes that could affect the DSS;
- recommendations for improvement.

Review output
The output from the management review should include any decisions and actions related to:

- improvement of the effectiveness of the DSS;
- update of the risk assessment and risk treatment plan;
- modification of procedures and controls that effect security, as necessary, to respond to internal or external events that can impact the DSS;
- resources needed.

8. DSS IMPROVEMENT

8.1 Objective

Effectiveness of physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE shall be reviewed and improved where necessary.

8.2 Policies

Policies shall define how effectiveness of security measures is maintained despite evolving threats and in consideration of possible deficiencies.

8.3 Security Measures

Continual improvement
The developer may continually improve the effectiveness of the DSS through the use of the security policy, security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review.

Corrective action
The developer should take action to eliminate the cause of nonconformities with the DSS requirements in order to prevent recurrence.

Preventive action
The developer should determine actions to eliminate the cause of potential nonconformities with the DSS requirements in order to prevent their occurrence.

The developer should identify changed threats and define preventive actions focusing on significantly changed risks.

9. CONTROL OBJECTIVES AND CONTROLS

9.1 Asset management

Security is involved with all kinds of assets but not all aspects of assets are in the scope of this DSS, e.g. QM (Quality Management), ESH (Environment, Safety, Health).

9.1.1 Overall objective

Assets shall be clearly identified with the type of protection (confidentiality, integrity, authenticity) assigned, and managed.

Every asset shall have an owner.

9.1.2 Responsibility for assets

Objective
Ownership and acceptable use of assets shall be defined and deployed.

Policies
DSD should define ownership and management of all assets.

Rules for the acceptable use of information and assets should be identified and documented in line with the classification policies.

Security measures
The most important assets within the scope of this annex are the TOE or parts of it. However, the form differs from segment to segment in the development phase of its life cycle.

Developer should consider the list of important assets given in example when defining assets.

Inventories of the assets should be available and maintained.

Owners should be identified and nominated for all assets in the different stages of the development. Performing ownership must be evident for all owners. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets.

The rules for the acceptable use of information and assets should be strictly enforced, and verified in internal audits.

Assets, particularly computers, and all other equipment and materials provided by the developer should be used for official purposes only, and only according to the rules set in the DSS and related documents.

Examples
For a typical Smart Card product (IC manufacturer) the following segments of the life cycle and forms of the TOE apply;

- Design – security concept, layout, net plan, software, data, bond out, design doc's (ADV-class)
- Mask production – pattern data, mask data, reticle
- Wafer production – reticle, wafer
- Wafer test – wafer, test program, (flash) application, application (EEPROM) data
- Assembly – wafer, modules/chips/package, test program, initialization data, embedded software
- Card/Inlay manufacturing – modules, cards
- Personalization – cards/inlays, embedded software, data
- Shipment – reticle, wafer, modules/chips, cards/inlays
- Rejects and scrap may appear in all segments and should be considered assets.

For typical products related to the Technical Domain hardware devices with security boxes, the following segments of the life cycle and forms of the TOE apply. Since this TD includes different product types, the segments of the life cycle would slightly differ:

- Design and Development Phase
- Manufacturing Phase
- Preparation Phase
- Component Supply*
- Assembly*
- Initialization
- Security Data Generation and Insertion*
- Storage distribution*
- Repair*
- Installation and Calibration Phase*
- Inspection and Calibration*
- Activation, Pairing or Coupling*
- Operational Phase
- Delivery Process preparation (Shipments)
- End of Life-Handling

*refer to Tachograph specific life cycle phases only (see Appendix 10 of Annex 1B of EC No 1360/2002- Generic Security Targets).

Rejects and scrap may appear in all segments and should be considered as assets. Delivery process preparation (Shipment) must be taken into account.

Important assets beside the TOE or parts of it are typically:

- Security: access control and alarm system, keys, access codes.
- Relevant information for the knowledge of the TOE: specifications, design documentation, guidance, source code, IC and embedded software representation, penetration tests results.
- Sensitive data used during the development phase of the TOE: keys, passwords, memory profile, integrity evidence.
- Information: databases, data files, contracts, system documentation, R&D information, archived information, production related data.
- Software: R&D tools, applications, system software, development tools, CM systems.
- Physical assets: computer equipment, communication equipment, removable media.
- Services: computing and communications services, general utilities (power, air conditioning, lighting), storage and shipment

An asset inventory includes:

- Type of asset
- Type of protection (confidentiality, integrity, authenticity, …)
- Format
- Location
- Backup information
- License information
- Protection level, criticality

The asset owner is responsible for:

- Ensuring that information and assets associated with processing facilities are appropriately classified;
- Defining and periodically reviewing access restrictions and classifications, taking into account applicable control policies.

Ownership is allocated for:

- All business processes
- Defined sets of activities
- Applications
- All defined sets of data
- Physical assets (premises, HW, networks etc.)

All information about assets are kept in appropriate databases.

9.1.3 Classification of information, data, and material

Objective
Assets shall receive an appropriate level of protection in line with their classification.

Policies
The developer shall have a classification policy.

The developer shall have predefined labelling and handling procedures for all used combinations of defined levels and information, data, and material implemented in accordance with the classification scheme adopted by the organization.

Security Measures
Assets should be classified according to an appropriate security level in terms of their criticality to the developer's organization and, particularly, to the intended area of application of any TOE concerned.

Classification relates to information, data, and material in any form:

- Hardcopy, e.g. documents, memos, presentations, drafts
- Electronic data, e.g. files, emails, software, development tools, CM systems, networks
- TOE and components (masks/reticules, wafer, dies, chips/modules, inlays, cards, demonstrators, samples, software etc.)

The classification scheme shall match with the classification as given in CEM AVA, paragraph 1975:

- Public information concerning the TOE (e.g. as gained from the Internet);
- Restricted information concerning the TOE (e.g. knowledge that is controlled within the developer organization and shared with other organizations under a non-disclosure agreement);
- Sensitive information about the TOE (e.g. knowledge that is shared between discreet teams within the developer organization, access to which is constrained only to members of the specified teams);
- Critical information about the TOE (e.g. knowledge that is known by only a few individuals, access to which is very tightly controlled on a strict need to know basis and individual undertaking);
- Very critical hardware design: The designs of modern ICs involves not only huge data bases but also sophisticated bespoke tools. Therefore, the access to useful data requires an enormous and time consuming effort which would make detection likely even with the support from an insider. If an attack is based on such knowledge the new level of “very critical design” has to be taken into account. It has to be decided in a case by case decision, if the knowledge cannot be gained in another way.

Classification should be in line with the factor “knowledge of the TOE” used to calculate an attack potential in Annex 7, Application of Attack Potential to Smartcards.

A level of protection in accordance with the developer’s classification policy should be associated with each asset.

The procedures for labelling and handling of information, data, and material should include, but are not limited to regulations regarding:

- Creation, Labelling, Issuing
- Distribution
- Dispatch / Transmission
- Retention / Storage
- Disposal / Destruction / Deletion

The rules for labelling and handling should be strictly enforced.

Where confidentiality is required, finished goods, semi-finished goods, rejected material, or parts of it that contain the TOE or its parts and that are no longer needed shall be destroyed in a way that remains cannot be used in any meaningful way that might affect confidentiality of the TOE

Access to restricted information, i.e. classified “sensitive” or “critical”, should only be granted on a need-to-know basis.

When a high level of security for especially critical material or operation is required, e.g. in case of classification “critical” or “or very critical”, the two-man rule (“four eyes principle”) should be applied as a control mechanism. Under this rule, all access and actions requires the presence of two authorized people at all times.

Information, data, and material considered sensitive, critical, or very critical shall be protected at any time.

The processes of destruction should be designed to provide full traceability of every piece of any tangible form of the TOE or its parts.

Examples
A typical classification scheme applies at least four levels of confidentiality, e.g.:

- open, public
- for internal use, company proprietary
- confidential, under NDA
- strictly confidential, company secret, top secret

Confidential electronic information is:

- distributed only to a defined group of people;
- transmitted electronically with appropriate end-to-end encryption (e.g., in 2012 German BSI requires at least 80 bits of entropy, i.e. 256 bit symmetric or 2048 bit asymmetric RSA key length);
- stored as encrypted file, in a secure container, or in a separated network;
- deleted by means of a wipe tool using at least 1 pass with random data pattern.

Destruction process:

- Wafer, single dies, and packaged chips are shredded in a rolling mill so that each edge of every die is cut 3 times.
- Masks/Reticules are re-etched in order to remove the pattern or shredded in a rolling mill.
- The destruction process of manifestations of the TOE is recorded on CCTV.
- Confidential and strictly confidential documentation of the TOE on paper or optical disks are shredded according to at least DIN 66399, Security Class 3:
  - Paper class P6 (max. 0,78 mm x 11 mm strips)
  - Optical disks class O6 (max. 0,5 mm² residual area)
  - Magnetic disks class T6 (max. 10 mm²)
  - Hard disk drives class H6 (max. 10 mm²)
  - Electronic disks (sticks, SSD) class E6 (max. 1 mm²)
- Files on re-writable data carriers (HDD, SSD, USB sticks) are wiped according to US DoD 5220.22-M or destroyed as described above.

9.1.4 Rules for preserving integrity and authenticity of assets

Objective
Assets shall be protected against alteration or unauthorized modification.

Policies
The developer shall have predefined handling procedures for all important assets in line with protection needs.

Approach to and deployment of configuration management shall be defined in a policy.

Whenever parts of the TOE are imported from external sources, import procedures should define how developer enforces integrity and authenticity of the imported parts.

Security measures
According to ALC_CMC an appropriate Configuration Management System shall identify and document the functional and physical characteristics of the TOE and its parts, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements in a way relevant for the different parts of the lifecycle. The Configuration Management System shall ensure the integrity of the TOE from the early design stages through all subsequent maintenance efforts, that the TOE is correct and complete before it is sent to the consumer and preventing unauthorized modification, addition, or deletion of TOE configuration items. (Detailed requirements for CM systems are defined in CC part 3, ALC.)

In the design phase of the TOE a configuration list shall clearly define all configuration items for a specific product together with the exact version of each item relevant for a specific version of the TOE and its parts, thereby allowing distinguishing the items belonging to different versions of the product.

During manufacturing the CM system shall ensure that only the planned processes and recipes are applied, that they are applied in the correct order, and that all manufacturing steps are documented to facilitate full traceability.

Where technical measures are not applicable, organizational measures should be implemented, e.g. four-eyes-principle.

For data in transit, detection measures should be implemented, e.g. check sum, hash value, signature.

If imported parts stem from other secure development environments, integrity, authenticity, and – where required – confidentiality shall be protected during transfer. The import from untrusted sources should involve inspection of the imported parts if modification of these parts has the potential to compromise integrity of the TOE. This applies in particular to the transfer of ROM code, EEPROM content, or software related to the TOE.

Examples
For the Technical Domain related to smart cards and similar devices: transfer security measures apply in particular to the transfer of ROM code or software related to EEPROM content or software related to the TOE.

For the Technical Domain related to hardware devices with security boxes: physical and logical security measures are defined. The transfer of logical security measures in particular applies to the transfer of initial firmware and software, loading of cryptographic keys, personalization and complementary software related to the TOE. The transfer of physical security measures in particular applies to initialization or Installation of the HW security features and maintain external enclosure out of visible damage until delivery (Example: manipulation traces).

9.2 Human Resources Security

9.2.1 Overall objective

The overall objective is to reduce the risk of theft, fraud or misuse of facilities by ensuring that employees, contractors, consultants, students, and third party users understand their responsibilities, and are suitable for the roles they are considered for.

9.2.2 Prior to employment

Objective
The developer shall grant access to assets only to trustworthy people.

The hiring and contracting process, respectively, shall ensure proper selection of team members.

Policies
DSD shall include policies for hiring and on-boarding which ensure careful selection of trustworthy staff.

Security Measures
Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant local laws, regulations and ethics, and proportional to the business requirements, the classification of the information and material to be accessed, and the perceived risks.

As part of their contractual obligation, the team members shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for security.

Contracts with all employees (permanent, temporarily, subcontractors, students etc.) shall contain a confidentiality clause which remains valid after expiration/termination of the contract; third party users respectively shall sign a non disclosure agreement (NDA).

The same security requirements shall apply to employees moving from other areas within developers organization.

Examples

Respecting privacy regulations, developer make reasonable effort to gain confidence in the integrity of the staff through:

- careful check of applications regarding completeness, conclusiveness, and authenticity,
- check of indicated references,
- criminal record check (“Clearance Certificate”, “Criminal Records Bureau check”, “Casier judiciaire”, “Polizeiliches Führungszeugnis” etc).

9.2.3 During employment

Objective
All team members shall be aware of information security threats and concerns and know their responsibilities and liabilities. They shall observe the rules and shall be equipped in order to support organizational security policies in the course of their normal work, and to reduce the risk of human error.

Policies
The developer shall have documents defining security roles and responsibilities of employees, contractors and third party users, in accordance with the organization's security policy (e.g. in job descriptions, project plans, contracts etc).

The approach to regular awareness training should be defined in a policy.

A policy should define monitoring measures implemented in order to detect irregular behaviour in line with local legislation.

Security Measures
Management shall require team members to apply security in accordance with established policies and procedures of the organization.

All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function. That can be face to face or online training. Records of the trainings should be kept, including date, attendances and content.

In order to identify security breaches monitoring records of security areas and secure networks, e.g. log files, should be analyzed in line with local legislation. There should be a formal disciplinary process for employees who have committed a security breach. Violations of security rules may be punished by disciplinary measures depending on the nature and gravity of the breach and its impact on confidentiality and integrity of the TOE, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required.

An initial and regular (annual) security training program should make the development team members aware of their responsibilities, e.g. handling of documents and information, behaviour in public, and encourage them to act pro-actively when problems occur. Process changes, learnings from security incidents and audits, and answers to frequently asked questions should be addressed in awareness trainings.

Examples
Developer's management ensures that team members:

- are properly briefed on their security roles and responsibilities prior to being granted access to sensitive areas, information, or information systems;
- are provided with guidelines to state security expectations of their role within the organization;
- achieve a level of awareness on security relevant to their roles and responsibilities within the organization;
- conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate working methods;
- continue to have the appropriate skills and qualifications;
- observe the rules;
- lead by example.

The disciplinary process is used as a deterrent to prevent team members violating organizational security policies and procedures, and any other security breaches.

9.2.4 Termination or change of employment

Objective
Team members leave developer (termination of contract or change of employment) in an orderly and controlled manner in order to maintain integrity and/or confidentiality of assets and/or information.

Policies
The developer shall have appropriate procedures for employment termination and change of job, including revocation of access rights.

Security Measures
Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned. This shall also apply to contracts with third party users.

All team members shall return all of the developer's assets in their possession upon termination of their employment contract or agreement. The same shall apply when they leave the developer's organization due to a change of job assignment.

Access rights (physical and logical) of all team members to developer's facilities shall be revoked without delay when no longer needed, particularly upon termination of their employment, contract or agreement, or adjusted upon change.

The employment change/termination process should be supported by a checklist for employees leaving employment in order to make sure that all relevant tasks, e.g. return of company properties, deletion of access rights are completed.

In case of suspension or dismissal due to disciplinary reasons, access rights shall be revoked immediately. The Security Manager shall be notified.

Where appropriate, team members should be notified about changed access rights.

9.3 Physical and environmental security

9.3.1 Overall Objective

Physical security shall prevent unauthorized physical access to the organization's premises, secure areas, delivery and loading areas, assets, and information which may impair integrity or - where required - confidentiality of TOE.

Integrity and - for security systems - availability (see also 9.8) of security relevant equipment shall be ensured to prevent loss, damage, theft, compromise, or loss of integrity of assets and security controls.

9.3.2 Physical security perimeter

Objective
Development areas where integrity and/or confidentiality of the TOE or its parts could be impaired shall be properly secured.

Protection of the premises shall have at least two lines of defence, a detection layer and a stop layer. These layers shall separate authorized from unauthorized people, including employees.

Policies
A security policies shall define the two layer security concept and detail the concerted function of the two layers.

Security Measures
Stop Layer and Detection Layer shall be implemented in a concerted and meaningful way. Evidence should be provided that the resistance time value of the stop layer exceed the reaction time of supporting forces.

All openings towards the secured development area (e.g. air condition, cable ducts) shall be protected in order to effectively prevent intrusion.

Where buildings are not solely used for developers' activities, e.g. shared with other users from the same organization (support functions, manufacturing, R&D), the layers shall separate the different activities.

In case that no physical manifestation of the TOE or its parts is handled and solely logical access to electronic data is present a stop layer may also be a logical one.

In case that a physical manifestation of the TOE or its parts has a "self protection" mechanism this can contribute to or be considered as a stop layer. Details are laid out in the respective Exhibit.

Examples
In a typical setup, the premises are located within a fenced site. The fence is protected with sensors (vibration, e.g. Perifone; motion, e.g. digital CCTV). Where the site may not be fenced an IR curtain can be deployed, or the outer skin of the building is monitored by digital CCTV with motion detection ("Telemat").

A Detection Layer consists of at least one of the following:

- Fence with sensor (vibration, ultrasonic, motion, etc.)
- IR curtain
- Digital CCTV with motion detection
- Wall with alarm tapestry or vibration sensor
- 24/7 guard post

A Stop Layer is a constructive measure which needs time to overcome:

- Concrete or brick stone wall, ceiling and floor;
- dry walling construction enforced with inside metal grid (> 8mm diameter, < 100 mm grid distance), with steel plate (> 3mm thickness), or alarm tapestry;
- windows in a stop layer are either protected with metal bars (> 8 mm diameter) or made with anti-burglary glass;
- door hardware must be properly installed, locked door blades fixed at floor and ceiling.

Development networks secured with strong access credentials and without TOE related data on local data carriers is considered a logical Stop Layer.

Controlled doors are strong (including frames), close automatically, and are monitored with magnetic contacts and CCTV.

Windows are secured with irremovable metal grid or with magnetic contacts and glass breakage sensors.

Air condition, cable ducts, etc. are protected with a welded metal grid.

9.3.3 Physical entry controls

Objective
Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Policies
An access control policy shall be in place, including regulations for visitors and contractors. Access shall only be granted on a need-to-know basis.

A policy shall define access regulations for service functions, e.g. housekeeping, facility management, cleaning staff.

Where applicable, policies shall detail access rights for officials and supporting forces, e.g. fire fighters.

Security Measures
Access requests shall be submitted in written or via an electronic work flow system.

A process shall be in place to ensure that access rights can only be granted after approval of responsible people, e.g. the manager of the applicant, the owner of the area, and the Security Manager.

Segregation of duty should ensure that setting access rights in the access control system is separated from producing and issuing badges.

The access control system should be tamper proof.

Tailgating should be prevented by technical or organizational measures, depending on size and nature of the site, and the associated risks.

In high security areas strong authentication should be implemented.

The access control system shall provide traceability. All access attempts shall be logged, and unauthorized access attempts should be analyzed and associated action should be applied in case of incident.

Where full traceability is required (depending on the nature of activities) automated mantrap with strong authentication shall be implemented.

In case physical keys are used to access the development area (i.e. where the key is the only access control measure) this area shall have a locking system independent from other areas. Such keys shall be kept secured in a safe place (e.g. key boxes, safe), with access only to authorized persons. Any withdrawal of a key shall be logged.

Examples
In a typical setup, access to the building is controlled by electronic badge access.

The entire access control system with badge (e.g. smart card), reader, and backbone system is tamper proof. It runs on a separated, secured network. Mutual authentication of badge and reader prevents unauthorized read of access credentials. Communication between the different components of the access control system are secured by an appropriate protocol (e.g. OSDP V2). Encryption and key management are secured by a Secure Access Module (SAM).

High security areas (e.g. laboratory, data center, Security Control rooms) have strong authentication, e.g. badge with PIN or biometrics.

Tailgating is prevented by turnstiles, either full height turnstiles or guard monitored standard turnstile.

Access to high security areas (e.g. design, security lab) is controlled by automated mantraps with strong authentication.

9.3.4 Securing offices, rooms and facilities

Objective
Physical security for offices, rooms, and facilities shall be protected against unauthorised access.

Any intrusion shall be detected immediately.

Policies
A Policy shall detail measures implemented to ensure detection and prevention of unauthorised access to offices, rooms, and facilities. This shall include clear security procedures and safety regulations as well as - where applicable - outsourcing.

Security Measures
Intrusion detection and alarm systems shall be designed and applied. The development area should be alarmed and locked when unattended.

Access controlled doors and emergency exits should be monitored with magnetic contacts and CCTV, and the restricted rooms should be monitored with motion detection.

Easily accessible windows should be protected against intrusion.

Detection and monitoring systems should be connected to a security center with 24/7 operation. The security center shall have an appropriate level of security. The connection of all security devices (e.g. intrusion detection, CCTV) to the security center shall be protected against tampering. All security relevant processes shall be audited.

Where the security centre is housing the primary systems for CCTV monitoring, intrusion, fire, alarm control and access control:

- The following processes fall under relevant security processes:
  - Access Control Management (rights to change badge access or create badges)
  - Activation and deactivation of security system
- The following processes are not considered as relevant security processes
  - View only access to CCTV
  - React only to security alarms with escalation to the company

Examples
Windows on ground floor or elsewhere reachable from a stand (roof, balcony, etc.) within 2.5 m are considered easily accessible.

9.3.5 Protecting against external and environmental threats

Objective
The security areas shall remain in a secure state and protect the TOE also in case of natural or man made disaster.

Policies
A disaster prevention and recovery policy is required, detailing the measures implemented to protect the TOE.

Security Measures
Appropriate physical protection against damage from fire, flood, and other forms of natural or man-made disaster should be designed and applied based on a risk assessment. Security systems like access control, CCTV etc. shall work even in case of natural or man-made disaster. This requirement also applies to logging and back-up systems.

9.3.6 Working in secure areas

Objective
Physical protection and guidelines for working in secure areas shall be designed and applied. Personnel shall be aware that information is only allowed to be shared on a need-to-know basis.

Policies
An access control policy based on need-to-know principle shall be developed, implemented, and maintained.

Security Measures
Access control rules and rights for each employee or visitor shall be clearly stated in an access control policy. Access controls are both logical and physical. Users and service providers shall be given a clear statement of the business requirements to be met by access controls.

People from external parties (e.g. customers, development partners, production partners, housekeeping, vendors, suppliers, carriers) shall not work in security areas without supervision of approved internals (e.g. host, owner of area, guard). This rule does not apply to externals who work as team members and are subject to the same security regulations as internals.

Vacant security areas shall be physically protected, e.g. with intrusion detection and fire alarm systems, and periodically checked.

Unauthorized use of photo and video cameras or audio recording equipment shall be prohibited.

9.3.7 Public access, delivery and loading areas

Objective
Access points such as delivery and loading areas, and other points where unauthorized persons may enter the premises shall be controlled and isolated from developer's processing facilities to avoid unauthorized access.

Visitors shall not get access to or insight into restricted areas or information unintentionally.

The TOE components shall be protected against tampering or theft during transit between physically separate secure areas.

Policies
The security policy shall consider that the design and layout of sites and premises should avoid high security areas next to public areas.

The security policy shall include a visitor regulation which has to be established, documented, and reviewed based on security requirements for access.

The security policy shall (if applicable) define measures to ensure that TOE components shall be protected against tampering or theft during transit between physically separate secure areas. Measures during transit shall correspond to the confidentiality and integrity classification.

Security Measures

Visitors
Visitors shall have only predefined, controlled access to the development environment. The routes and walkways designated to visitors should be designed to ensure that visitors will not see restricted areas or information unintentionally. Procedures applying to visitors should include:

- A documented application process for visits defining who is authorized to receive visitors and who is entitled to approve.
- A registration procedure ensuring that the visitor's identity is verified against an official government issued document (picture ID). Visitor information, the contact person in the development environment, time in and time out and the reason for the visit are recorded.
- Visitors display their visitor badge during the entire visit.
- Visitors are escorted at all times within the development environment either by a person from the development environment or by security personnel.

Delivery and shipment
Areas for incoming deliveries and outgoing shipments should be separated; separation may be physically or temporarily.

Delivery and shipping areas shall be designed in a way that no carrier personnel could gain access to other parts of the premises. External doors of these areas should be secured when internal doors are opened (interlock).

Carriers' drivers and trucks should be listed with name, photo, signature, make, and license plate number. Only listed trucks and drivers may get access to the premises.

Deliveries to developer's premises should be announced. The carrier should not get access to developer's security areas, including shipping area and warehouse, but stay in delivery and loading area.

Delivery and loading area shall be monitored by CCTV. The recordings shall provide clear pictures enabling developer to identify any unintended unloading and loading.

Incoming material shall be registered on entry, and inspected for potential threats before delivery to the point of use.

Transportation
There are no particular requirements for physical transfer of materials within a physically secured area except that transfer shall be logged in order to provide full traceability.

The whole transport chain from initial development area to shipment of the TOE to the customer shall be controlled. Transport shall be monitored for security violations and any incidents shall be responded to and acted upon immediately.

At certain stages in the life cycle the TOE may be self-protecting according to CC part 1 line 136. In that case transportation security is not required if security measures are in place enabling recipient to undoubtedly identify origin of shipment.

The TOE components shall be protected against tampering or theft during transit between physically separate secure areas. The protective mechanism shall enable the recipient to detect if tampering or theft has taken place.

A recipient should be provided with all information necessary to verify the integrity and authenticity of the shipment. The following information should be included:

- Number of boxes
- Seal number(s) of transport box(es)
- Number of pieces packed
- Route and schedule
- Drivers name, truck license plate number

In order to prevent attacks shipment information should be encrypted.

Upon receipt the recipient shall check the shipment without delay and acknowledge the integrity and authenticity status. In the event of a violation of shipment integrity or authenticity this acknowledgement shall be kept together with the original shipping notification.

Examples
During transportation, the TOE is attended at any time except while locked in an airplane.

For ground transportation, the following rules are deployed:

- TOE or parts of it are packed in sealed transport boxes with unpredictable seal number (seal, plumb, or security tape)
- transport in a vehicle (commercial van, truck) with locked cargo area
- point-to-point transport without additional payload or hub/relation
- Two-man rule is applied during the entire transportation and the vehicle is not unattended at any time
- the transport is equipped with mobile phone and GPS based surveillance

9.3.8 Equipment security

Objective
Integrity and – for security systems - availability of security relevant equipment shall be ensured to prevent loss, damage, theft, compromise, or loss of integrity of assets and security controls.

Policies
A policy shall define handling and placing of security relevant equipment in order to protect against failures which could affect availability of those equipment, and interception or damage.

Security Measures
Security relevant equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Security equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

Power and telecommunications cabling carrying sensitive data or supporting security relevant information services shall be protected from interception or damage.

Equipment should be correctly maintained to ensure its continued integrity and – for security systems - availability.

Security measures should be applied to off-site equipment (Laptop, Mobile Phone, Handheld, Data carrier) taking into account the different risks of working outside the developer's premises. Utilization of such equipment shall be limited to activities not directly associated to the TOE and shall be authorized by management.

All items of equipment containing storage media shall be checked to ensure that any sensitive data has been securely removed prior to disposal or re-use outside the developer’s premises.

Equipment, information or software shall not be taken off-site without prior authorization.

Examples
Equipment is located in areas minimizing unnecessary access into security areas. It is positioned to prevent unauthorized viewing.

Network cabling is protected from unauthorized interception or damage by avoiding routes through public areas. Cable run in cable ducts.

Access to switches and patch panels is restricted.

Classified information, data, and material is removed before maintenance. All maintenance is logged with date, time, and personnel involved.

A procedure for the permission to take company properties off-site is defined and deployed. Spot checks to detect unauthorized removal are conducted in accordance with relevant legislations and regulations.

9.4 Communications and operations management

9.4.1 Overall objective

Operations and communication related to TOE as well as to supporting infrastructures and resources shall be protected against internal and external threats.

9.4.2 Operational procedures and responsibilities

Objective
The TOE related operations shall be protected against unintentional or deliberate misuse of processing facilities or incorrect operations execution.

Infrastructure used to protect integrity and/or confidentiality of the TOE shall be secured.

Policies
Operating procedures shall be documented, maintained, and made available to all users who need them.

Formal management responsibilities and procedures should be in place to ensure satisfactory control of equipment, software, or procedures, and all related changes.

A procedure shall define the level of separation between development, test and operational environments, and describe the controls implemented.

Security Measures
Developer should deploy an appropriate level of separation between development, test, and operational environment.

The correct usage of processing equipment and of operations execution should be facilitated by up-to-date operating procedure documentation.

Processing facilities should be subject to strict change management processes; changes should need authorization by management. When changes are made, an audit log containing all relevant information should be retained.

Utilizing or modifying assets without authorization or detection should be prevented by segregation of duties and areas of responsibilities. The following items should be considered:

- The initiation of an event should be separated from its authorization.
- The possibility of collusion should be considered in designing the controls.
- Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered.

Examples
Operating procedures and documented procedures for system activities are formal documents.

Documented procedures are available for system activities associated with information processing and communication facilities, such as computer start-up and shut-down procedures, back-up, equipment maintenance, media handling, computer room and mail handling management, and safety.

The operating procedures specify the instructions for the detailed execution of each job.

Change controls consider the following items:

- Identification and recording of significant changes;
- Planning and testing of changes;
- Assessment of the potential impacts, including security impacts, of such changes;
- Formal approval procedure for proposed changes;
- Communication of change details to all relevant persons;
- Fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.

Access to the access control system is segregated from handling of physical badges, e.g. assigned to HR and security guards, respectively.

9.4.3 Third party service delivery management

Objective
When third party services are used confidentiality and/or integrity of the TOE and its part shall be preserved.

Policies
Contract and vendor management policies shall define roles and responsibilities for managing the relationship with third parties.

Security Measures
The responsibility for managing the relationship with a third party should be assigned to a designated individual or a service management team.

Service Contracts and Statements of Work should pass the developer’s internal approval process. The Security Manager shall be involved and any feedback considered.

Third party services should be monitored and reviewed in order to check that security terms and conditions of the agreements are being adhered to, and that security incidents and problems are managed properly. A report should be kept as evidence.

9.4.4 System planning and acceptance

Objective
Systems planning shall minimize the risks of system failures for all systems supporting confidentiality and/or integrity of the TOE and its part.

Policies
A planning process for communication and operation systems shall be defined and documented.

Test procedures and acceptance criteria for new processing systems, upgrades, and new versions shall be established.

Security Measures
The use of resources should be monitored and tuned to ensure the required system availability and performance.

New processing systems, upgrades, and new versions should be tested prior to acceptance ensuring that all acceptance criteria have been satisfied. Migration into production should require formal acceptance. The Security Manager shall be involved and heard.

Acceptance may include a formal certification and accreditation process to verify that the security requirements have been properly addressed.

9.4.5 Protection against malicious and mobile code

Objective
The integrity of systems and software supporting TOE related information shall be protected against malicious code where applicable.

Policies
A policy shall prohibit the use of unauthorized software.

A policy shall define compulsory protective measures to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium.

Management procedures and responsibilities shall be defined for malicious code protection on systems, including training in their use, alerting, reporting, and recovering from malicious code attacks.

A security policy shall define authorized mobile code operations.

Security Measures
Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.

Computers and all other equipment and materials provided by the developer shall be used for company purposes only; exceptions may be defined for smart phone use. Downloading or storing unapproved software or data shall not be allowed.

Regular reviews of the software and data content of connected systems supporting critical business processes shall be conducted; the presence of any unapproved files or unauthorized amendments should be formally investigated.

Malicious code detection and repair software should be installed and regularly updated in order to scan computers and media as a precautionary control, or on a routine basis.

Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from execution.

Access to mobile code on external web sites shall be restricted, e.g. on proxy servers. On the client, with the restricted/trusted sites mechanism of the browser, access to websites containing mobile code should only be granted after formal approval.

9.4.6 Back-up

Objective
Integrity, availability, and – where required – confidentiality of TOE related information and security systems (at least TOE related data, access control and administrator log files) shall be ensured when a back-up system is used.

Policies
A documented procedure approved by the Security Manager shall define secure back-up creation, storage, and destruction operations, ensuring the same level of security as for the original data.

Security Measures
Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure while maintaining confidentiality and integrity of the TOE and its part.

Back-up arrangements should be regularly tested to ensure that they meet the requirements of the agreed back-up policy.

For critical systems, the back-up arrangements should cover all system information, applications, and data necessary to recover all TOE related and security systems in the event of a disaster.

Examples

The retention period for essential information and any requirement for archiving information permanently are determined.

Regular daily, weekly, and monthly back-up on data carrier (HDD, DVD, tape) is used by small entities. Large entities usually back-up data via online systems to remote locations or mirror data on redundant hot systems.

The security environment hosting back-ups provides the same level of security as the operational environment.

9.4.7 Network security management

Objective
Network security shall ensure adequate protection of TOE related data and information, and security infrastructure.

Policies
Developer shall specify network security in terms of network architecture and preventive and detective measures.

A policy shall restrict network traffic through the entry point into the development area’s network to its minimum.

Security Measures
Network infrastructure security shall be based on implementation of the following security measures:

- Access restriction to authorized people only.
- Entry point control, restricting the traffic to a minimum.
- Separation from other network either physically or by VLAN technologies, protected by access control measures and appropriate firewall rules.
- Physical separation of hardware (e.g. server, firewall, router, patch panel, etc.) and administration into properly secured premises consistent with the security level of the development area.
- Strong authentication scheme defined for network access.
- Secured configuration of development machines with a controlled, restrictive user security policy that prevents the installation of additional, unauthorized functionality.
- Use of a mechanism between the corporate/public network boundary and the development area IT systems that provides up-to-date commercial grade protection against logical attacks.
- No wireless connectivity for development networks.

Network controls implementation should also consider the following items:

- Operational responsibility for networks separated from computer operations, e.g. network operation centre for administration of network devices and local administration of servers;
- Special controls to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks, and to protect the connected systems and applications; special controls to maintain the availability of the network services and computers connected as far as security systems are concerned;
- Appropriate logging and monitoring to enable recording of security relevant actions;
- Management activities coordinate both, to optimize the service to the organization and to ensure that controls are consistently applied across the processing infrastructure.
- Members of the development environment should not have administrator rights on the IT systems which they work with.

It should not be possible to view and/or modify configuration items from outside the defined development area, even from within the corporate network.

Access to development networks should be limited to hardened client supplied by the developer. Development networks processing restricted information shall only permit remote access on hardened client specifically intended for this purpose via secure VPN. Development networks processing sensitive, critical, or very critical information shall not allow remote access from outside of the development network.

Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or are outsourced.

The developer should segregate duties in IT administration (network, server, client, application administration). Administrator log files should be kept secured out of reach of the administrator.

Examples
In a typical setup the network is protected with:

- Application layer firewalls with restrictive rules
- Network admission control
- Intrusion detection/prevention systems
- Virus/malware protection

Common services (AD, DNS, license servers, etc.) are hosted in a DMZ. Network, server, and client administration is segregated.

Access to development networks is only possible with Thin Clients (terminals) or hardened clients which effectively prevent copying network content (e.g. no I/O except monitor, keyboard, and mouse).

9.4.7 Media handling

Storage media is used to both store data and to transport it from one location to another. Media may be tapes, HDD, USB Sticks, CD/DVD/BD, smartphones, smart cards, and any other data carrier.

Objective

In order to protect integrity and/or confidentiality of TOE related data and information, all media shall be protected against unauthorized disclosure, modification, removal, theft, destruction or damage.

Policies

Appropriate operating procedures should be established to protect documents, computer media, mobile devices, input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction.

Where confidentiality and/or integrity are required, procedures shall be in place for the management of removable media.

All procedures and authorization levels should be clearly documented.

Formal procedures for the secure disposal of media shall minimize the risk of sensitive information leakage to unauthorized persons. The procedures for secure disposal of media containing classified information should be commensurate with the classification of that information.

Security Measures

Media should be controlled and physically protected. Security measures should include appropriate media labelling, storage, safe transportation, disposal and handling that are necessary and vital to protect all forms of media used for the storage of data.

Classified data (restricted, sensitive, and critical) shall be encrypted while stored on movable data carrier and during transit.

Media shall be disposed of securely and safely when no longer required, using formal procedures.

Permission for removable media should be granted only if need is evident. Media should be stored in a safe, or a secure environment, in accordance with developer’s specifications. Registration of removable media and a removal authorization process should be implemented in order to reduce opportunity for data loss and provide an audit trail.

Media containing non-public information should be stored and disposed of securely. Service providers for the collection and disposal services for papers, equipment and media should be selected carefully.

Disposal of sensitive items should be witnessed by developer’s employees and logged as appropriate in order to maintain an audit trail.

When accumulating media for disposal, consideration should be given to the aggregation effect, which may turn a quantity of non-sensitive information into sensitive information.

Examples

An inventory provides the current status of all data media used for TOE related activities.

An approval process for removable media drives ensures that permission is granted only if need is justified. Records of removals are kept and an audit trail is maintained.

All media are stored in a safe when not in use.

Discarded optical disks (CD, DVD, BD) are shredded.

HDD are sanitized according to DoD 5220.22-M (3 passes) for further use within the organization.

The destruction process is logged and recorded on CCTV. Disposal of sensitive items is witnessed by developer’s trustworthy employees.

9.4.9 Exchange of information

Objective
Integrity and - where required - confidentiality of information and data shall be maintained while exchanged within an organization or with any external entity.

Policies
Formal exchange policies, procedures, and measures shall be defined and deployed in order to protect the exchange of information through the use of all types of communication facilities.

Security Measures
Data transfer to/from secured networks shall only be possible via secure mechanism with authorised access accounts. Appropriate measures shall be implemented to separate the external networks from the secured networks.

Where confidentiality and integrity of the TOE and its parts is required, transfer of related information and data shall be encrypted and signed. If only integrity of the TOE and its parts is required, transfer of related information and data shall be signed.

Agreements should be established for the exchange of information and software between developer and external parties. Developer's policies, procedures, and standards should be referenced in such exchange agreements. The security content of any agreement should reflect the sensitivity of the business information involved.

Information involved in electronic messaging should be appropriately protected. Security considerations should include the following items:

- Protecting messages from unauthorized access (password, encryption) or modification;
- Ensuring correct addressing and transportation of the message;
- Ensuring authenticity of the message, i.e. sender/author of the message should be unambiguous;
- Strong authentication restricting access from publicly accessible networks, e.g. client certificate and VPN.

For shipment of data carrier and documents only company approved couriers should be used.

Examples
Exchange of documents or hardcopies is protected by utilization of locked containers or delivery by hand.

Tamper-evident packaging reveals any attempt to gain access.

In case of high security requirements, splitting of the consignment into more than one delivery and shipping on different routes can protect effectively.

9.4.10 Electronic commerce services

Not applicable

9.4.11 Monitoring

Objective
Unauthorized processing activities shall be detected.

Policies
A policy shall detail monitoring measures, particularly logging and assessment of log files.

Security Measures
To allow detection of unauthorized processing activities, and to assist investigations, the following log files shall be produced and kept for a defined period of time:

- User activities, exceptions and information security events.
- System administrator and system operator activities.
- Denied login attempts or security breaches (by enabling the Security Event log function of all clients).
- Network related system activities from domain controllers, firewalls, or proxy servers.

Logging facilities and log information shall be protected against tampering and unauthorized access. The system administrator log files should be kept out of reach of the respective administrator or system operator, respectively, and checked at least monthly for suspicious activities.

Examples
Payment schemes require three months online, one year offline retention period for audit log files.

9.5 Access control to information systems

9.5.1 Overall Objective

Access (logical and physical) to information systems including access to business processes, to networks, to operating systems, to applications, and to information shall be controlled and restricted on a need-to-know basis.

Users, user roles, and user responsibilities shall be managed and controlled.

9.5.2 Business requirement for access control

Objective
Access to information, information processing facilities, and business processes shall be controlled on the basis of security requirements.

Policies
An access control policy shall be established, documented, and regularly reviewed based on business requirements (security needs to protect confidentiality and/or integrity of TOE) for access. This policy shall detail access control rules for every role (user or group of users).

Security Measures
Access shall be granted only on a need-to-know basis.

Access control roles for both, access to premises and access to systems, should be segregated, e.g. access request, access authorization, and access administration.

Examples
An access control policy takes into account:

- security requirements of developers business activities;
- policies for information dissemination and authorization, e.g. the need-to-know principle and security levels and classification of information;
- consistency between the access control and information classification policies of different systems and networks;
- relevant legislation and any contractual obligations regarding protection of access to data or services;
- management of access rights in a distributed and networked environment which recognizes all types of connections available.

Roles in the access authorization process are segregated. Requests are approved by the applicant's manager and the system and/or data owner, authorization is implemented by a security manager (physical access) or an IT administrator (logical access), respectively. The access control system is managed by its owner (security manager, application owner, system administrator).

9.5.3 User access management

Objective
Only authorized users shall be able to access information systems.

Policies
A policy regarding user access management shall be established and documented. It details how access rights and privileges are granted and the roles used.

A policy regarding password quality shall be established and documented.

Security Measures

The procedures shall cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer need access to information systems and services. Special attention shall be given to the need to control the allocation of privileged access rights.

All users shall have a unique identifier for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user. This is mandatory for all types of users (including technical support personnel, operators, network administrators, system programmers, and database administrators).

There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.

The access control procedure for user registration and de-registration should include:

- using unique user IDs (e.g. user accounts) to enable users to be linked to and held responsible for their actions; the use of group IDs shall only be permitted where they are necessary for business or operational reasons, and shall be approved and documented; responsible persons for such group IDs shall be named;
- checking that the user has authorization from the system owner for the use of the information system or service; separate approval for access rights from management may also be appropriate;
- checking that the level of access granted is appropriate to the business purpose and is consistent with organizational security policy, e.g. it does not compromise segregation of duties;
- giving users a written statement of their access rights;
- requiring users to sign statements indicating that they understand the conditions of access;
- ensuring service providers do not provide access until authorization procedures have been completed;
- maintaining a formal record of all persons registered to use the service, e.g. Active Directory;
- immediately removing or blocking access rights of users who have changed roles or jobs, or left the organization;
- periodically checking for, and removing or blocking, redundant user IDs and accounts;
- ensuring that user IDs are not re-issued to other users.

The allocation and use of privileges shall be restricted and controlled.

Multi-user systems that require protection against unauthorized access shall have the allocation of privileges controlled through a formal authorization process.

The following steps shall be considered:

- the access privileges associated with each system, e.g. operating system, database management system and each application, and the users to which they need to be allocated shall be identified;
- privileges shall be allocated to users on a need-to-use basis
- an authorization process and a record of all privileges allocated shall be maintained. Privileges shall not be granted until the authorization process is complete;
- the development and use of system routines should be promoted to avoid the need to grant privileges to users;
- the development and use of programs which avoid the need to run with privileges should be promoted.

The allocation of passwords shall be controlled through a formal management process. This process shall consider the following requirements:

- when users are required to maintain their own passwords they should be provided initially with a secure temporary password, which they are forced to change immediately;
- establish procedures to verify the identity of a user prior to providing a new, replacement or temporary password;
- temporary passwords shall be given to users in a secure manner; the use of third parties or unprotected (clear text) electronic mail messages shall be avoided;
- temporary passwords shall be unique to an individual and shall not be guessable;
- passwords shall never be stored on computer systems in an unprotected form;
- default vendor passwords shall be altered following installation of systems or software.

Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means, should be used.

Systems for managing passwords should be interactive and ensure quality passwords.

The password management system should:

- store password files separately from application system data;
- store and transmit passwords in protected (e.g. encrypted or hashed) form.

Management shall review users' access rights at regular intervals using a formal process. The review of access rights shall consider the following guidelines:

- users' access rights should be reviewed at regular intervals, e.g. a period of 6 months;
- users' access rights should be reviewed after any changes, such as promotion, demotion, or termination of employment;
- privilege allocations shall be checked at regular intervals to ensure that unauthorized privileges have not been obtained;
- changes to privileged accounts shall be logged for periodic review.

Examples
Inappropriate use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) can be a major contributory factor to the failures or breaches of systems.

Passwords are a common means of verifying a user's identity before access is given to an information system or service according to the user's authorization. Other technologies for user identification and authentication, such as biometrics, e.g. fingerprint verification, signature verification, and use of hardware tokens, e.g. smart cards, are available, and are considered - where appropriate – to replace or complement passwords.

It is necessary to regularly review users' access rights to maintain effective control over access to data and information services.

Users are required to sign a statement to keep personal passwords confidential; this signed statement is included in the terms and conditions of employment.

9.5.4 User responsibilities

Objective
User responsibilities for maintaining effective access control shall be clearly defined and users shall be aware of their responsibilities.

Policies
A policy shall detail users’ responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

A password policy shall require users to follow good security practices in the selection and use of passwords.

Security Measures
Developer shall follow good security practices in the selection and use of passwords.

In the password policy all users shall be required to:

- keep passwords confidential;
- avoid keeping a record;
- change passwords at regular intervals or whenever there is any indication of possible system or password compromise;
- select quality passwords;
- change temporary passwords at the first log-on;
- do not include passwords in any automated log-on process, e.g. stored in a macro or function key;
- do not share individual user passwords;
- do not use the same password for business and non-business purposes.

Users shall ensure that unattended equipment has appropriate protection.

Where relevant, all users shall be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection.

Users should be advised to:

- terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;
- log-off mainframe computers, servers, and office PCs when the session is finished (i.e. not just switch off the PC screen or terminal);
- secure PCs or terminals from unauthorized use by a key lock or an equivalent control, e.g. password access (CTRL-ALT-DEL in Windows), when not in use;
- protect data stored on movable equipment by encryption of the persistent storage; where data is not encrypted movable equipment (notebook) should be secured by physical measures (e.g. with cable lock Kensington lock or kept in a locked cabinet) when not in use;
- keep data media locked unless encrypted.

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted to reduce the risk of a security breach, fraud, and information theft facilitated by unattended documents or media.

The clear desk and clear screen policies should provide guidance to all users regarding handling of documents, data, and media according with respect to their classification.

Examples
The Password Policy requires users to:

- select quality passwords with sufficient minimum length (at least 8 characters), e.g. at least one character from 3 out of the following 4 categories:
  - Lower case characters (a...z)
  - Upper case characters (A...Z)
  - Numerical characters (0...9)
  - Special characters (!"$%&/()=?*....);
- keep passwords confidential;
- store passwords securely utilizing an approved password safe;
- change passwords at regular intervals, e.g. every 90 days;
- change temporary passwords at the first log-on;
- do not include passwords in any automated log-on process, e.g. stored in a macro or function key;
- do not share individual user passwords;
- do not use the same password for business and non-business purposes.

Unattended clients or workstations are protected by an activated, locked screensaver.

Equipment installed in user areas, e.g. workstations or file servers, has specific protection from unauthorized access when left unattended for an extended period.

9.5.5 Network access control

Objective
Unauthorized access to networked services shall be prevented.

Policies
A policy regarding network access management shall be established and documented. It details the network architecture, network connections, network access control and other security measures.

Dedicated processes and guidelines for business partner access and interconnections with/to business partners shall be defined and documented.

Security Measures
Only devices controlled by developer shall be able to connect to the network.

It shall be ensured that user access to networks and network services can not compromise the security of the network services by:

- appropriate interfaces between the organization's network and networks owned by other organizations, and public networks;

- appropriate authentication mechanisms for users and equipment;
- control of user access to information services.

Firewall Syslog messages should be analyzed regularly and actions are taken when necessary.

Where remote access to developers' networks is permitted appropriate authentication methods shall be used to control access by remote users. Where confidentiality of sensitive, critical or very critical information is required, remote access to security networks, particularly networks where TOE or its parts or related design information is handled, shall not be possible.

Where confidentiality of restricted information or only integrity is required remote access may be allowed with suitable security measures ensuring integrity and if applicable confidentiality on the same level of network security as in the developer's premises.

Automatic equipment identification should be used as a means to authenticate connections from specific locations and equipment. This control should be complemented with other techniques to authenticate the equipment's user. Equipment identification shall only be applied in addition to user authentication, not as replacement.

Physical and logical access to diagnostic and configuration ports shall be controlled. Ports, services, and similar facilities installed on a computer or network facility which is not specifically required for business functionality should be disabled or removed.

Groups of information systems, information services, or users should be segregated on networks, e.g. in different security zones or network branches.

Where confidentiality and/or integrity are requirements, the following high-level requirements shall apply to all security zones or network branches of all levels;

- All interconnections between security zones and network branches shall be planned and controlled by a central authority, involving the Security Manager;
- The interconnection of distributed parts of a security zone or network branch shall be encapsulated/protected by the use of secure network techniques, e.g. secure VPN;
- Responsibility for the interconnections and for the data processed within the security zones themselves should be segregated to deploy four-eye principle (This means that it shall not be possible for a single person to establish a data channel outbound or inbound).

For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control regulations and requirements of the business applications.

The network access rights of users shall be maintained and updated as required by access control regulations.

The connection capability of users can be restricted through network gateways that filter traffic, e.g. by means of pre-defined tables or rules (application layer firewall).

Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications. Routing controls shall be based on positive source and destination address checking mechanisms. Security gateways should utilize at least either:

- firewalls to validate source and destination addresses on the network layer;
- proxy server to validate source and destination addresses on application layer;
- SOCKS proxy server for user authentication.

Shared networks, especially those extending across organizational boundaries, may require additional routing controls. This particularly applies where networks are shared with third party (non-organization) users.

Examples
Network access is controlled by Network Access Control (NAC) systems, allowing access only for managed devices. NAC can be basic (using a local ID of the device, eg MAC address) or strong (using machine certificate and computer account in active directory).

Developer's network is separated from other networks by a DMZ with firewalls at either end.

Cascading networks ensures that access to a network is granted from an appropriate security level. Connected clients are member of the respective Windows Client Domain and can be identified via certificates.

Equipment identification is used if it is important that the communication can only be initiated from a specific location or equipment. The identifier indicates whether or not this equipment is permitted to connect to a certain network. It may be necessary to consider physical protection of the equipment to maintain the security of the equipment identifier.

Employees and business partners with notebooks installed and managed by developer's IT (machine certificates) are enabled to get full network access to developer's intranet, file server, and Exchange Server while business partners and contractors without developer's equipment get only restricted access to some applications hosted in the DMZ.

Potential controls for the access to diagnostic and configuration ports include the use of a key lock and supporting procedures to control physical access to the port. An example for such a supporting procedure is to ensure that diagnostic and configuration ports are only accessible by arrangement between the manager of the computer service and the hardware/software support personnel requiring access.

9.5.6 Operating system access control

Objective
Unauthorized access to operating systems shall be prevented.

Policies
A policy shall be established and documented describing the measures taken to prevent unauthorized access to operating systems.

Security Measures
Security facilities shall be used to restrict access to operating systems to authorized users. The facilities should be capable of the following:

- authenticating authorized users, in accordance with a defined access control policy;
- recording successful and failed system authentication attempts;
- recording the use of special system privileges;
- issuing alarms when system security policies are breached.

Access to operating systems shall be controlled by a secure log-on procedure.

The procedure for logging on to an operating system shall be designed to minimize the opportunity for unauthorized access. The log-on procedure should therefore disclose the minimum of information about the system, in order to avoid providing an unauthorized user with any unnecessary assistance.

The use of utility programs that might be capable of overriding system and application controls shall be restricted on a need-to basis and tightly controlled.

A time-out facility should clear the session screen and also, possibly later, close both application and network sessions after a defined period of inactivity. The time-out delay should reflect the security risks of the area, the classification of the information being handled and the applications being used, and the risks related to the users of the equipment.

Connection time controls should be considered for sensitive computer applications, e.g. those with access to the TOE and its parts in order to provide additional security for high-risk networks or applications.

Examples
A limited form of time-out facility is the password protected screensaver which is part of the Windows installation. It clears the screen and prevents unauthorized access but does not close down the application or network sessions.

9.5.7 Application and information access control

Objective
Integrity and - where required - confidentiality of TOE related data and information, and security systems shall be protected through effective access control to applications and information.

Policies
A policy shall detail the measures taken to restrict access to applications and information, and to isolate systems with sensitive, critical, or very critical content.

Security Measures
Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policies.

Need-to-know principle shall be implemented throughout the entire application landscape, e.g. project specific access rights, restricted access to work shares.

Systems with sensitive, critical, or very critical content shall have a dedicated (isolated) computing environment.

Applications and systems with sensitive, critical, or very critical content (e.g. development networks, IT Administration Network) shall not run in shared environments. The necessary shared services (e.g. Active Directory, Netinstall, license server, drop box) shall be installed in a DMZ. Data should be transferred via drop box mechanisms.

9.5.8 Mobile computing and teleworking

Objective
TOE related data and information, and security systems shall be appropriately protected when using mobile computing and teleworking facilities.

Policies
A policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing (laptop, handheld devices) and communication facilities (smart phones etc.).

A policy, operational plans and procedures shall be developed and implemented for remote access and teleworking activities if applicable.

Security Measures
Where confidentiality of sensitive, critical, or very critical information is required, mobile computing of the TOE or its parts or related design information shall not be possible.

Where confidentiality of restricted information or only integrity is required mobile computing may be allowed with suitable security measures ensuring integrity and if applicable confidentiality on the same level of network security as in the developer’s premises.

Teleworking with access to the TOE or its parts, TOE related information, and related security systems shall only be allowed for environments with public or restricted content in absence of sensitive, critical, or very critical content. The teleworking environment (premises, IT etc.) shall meet all requirements related to integrity and - where applicable - confidentiality set in this document. If teleworking is permitted processes shall be in place to ensure integrity during all teleworking activities.

Care should be taken when using mobile computing facilities in public places (even inside the premises), meeting rooms and other unprotected areas outside of the organization’s premises. Protection should be in place to avoid unauthorized access to or disclosure of the information stored and processed by these facilities, e.g. using cryptographic techniques.

Teleworking uses communications technology to enable staff to work remotely from a location outside of the developers` environment. Mobile devices must be protected against logical attacks during access of external networks to the same extent as provided by the developers` network.

Examples

Remote access from the home office to developer's office environment is possible in order to check email and to use common office tools. Access to sensitive specifications, application notes etc. is not permitted.

9.6 Information systems acquisition, development and maintenance

9.6.1 Overall Objective
Security shall be an integral part of information systems. IT systems shall be secured to a level ensuring integrity and confidentiality of the TOE, and safeguarding availability and proper operation of security systems.

Information systems include operating systems, infrastructure, business applications (e.g. development environments, configuration management systems), and services, either off-the-shelf products or user-developed applications.

9.6.2 Security requirements for information systems (informative)

Objective
Security requirements should be identified and agreed upon prior to procurement of IT systems. Security should be an integral part of procurement requirements for information systems.

Policies
A procurement policy should define the steps necessary to mitigate risks from IT systems (hardware and software) in use.

Software development, implementation, and utilization of applications developed by or on behalf of developer should be detailed.

Installation and verification of off-the-shelf products should be defined.

Security Measures
All security requirements should be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system.

Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.

When products are purchased, a formal testing and acquisition process should be followed. Contracts with the supplier should address the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement the risk introduced and associated controls should be reconsidered prior to purchasing the product. Where additional functionality is supplied and causes a security risk, this functionality should be disabled or the proposed control structure should be reviewed.

9.6.3 Correct processing in applications

Objective
Errors, loss, unauthorized modification, or misuse of information in IT systems shall be prevented.

Integrity and/or confidentiality of the TOE and its parts shall be ensured.

Policies
A policy shall detail measures implemented to ensure integrity and authenticity of data related to the TOE or to proper operation of security systems.

Security Measures
Appropriate controls should be designed into applications, including user developed applications, to ensure correct processing. These controls should be determined on the basis of security targets, other security requirements, and risk assessment. They should include the validation of input data, internal processing, and output data.

Typically, systems and applications are constructed on the assumption that having undertaken appropriate validation, verification, and testing, the output will always be correct. However, this assumption is not always valid; i.e. systems that have been tested may still produce incorrect output under some circumstances.

<u>Input data validation (informative)</u>
Data input to applications with impact on security and/or integrity of the TOE and its parts should be validated to ensure that this data is correct and appropriate.

Automatic examination and validation of input data should be considered, where applicable, to reduce the risk of errors and to prevent attacks.

<u>Control of internal processing (informative)</u>
The design and implementation of applications should ensure that the risks of processing failures leading to a loss of integrity or confidentiality are mitigated. Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate.

Message integrity (informative)
The integrity of electronic mail communication should be ensured by using the encryption and signing functionality based on suitable cryptographic algorithms and appropriate protocols.

Output data validation (informative)
Data output from an application should be validated to ensure that processing of stored information is correct and appropriate to the circumstances.

Examples
Checking input of data typically includes the following steps:

- dual input or other input checks, such as boundary checking or limiting fields to specific ranges of input data, to detect errors;
- periodic review of the content of key fields or data files to confirm their validity and integrity;
- inspecting hard-copy input documents for any unauthorized changes (all changes to input documents should be authorized);
- procedures for responding to validation errors;
- procedures for testing the plausibility of the input data;
- defining the responsibilities of all personnel involved in the data input process;
- creating a log of the activities involved in the data input process.

Control of internal processing may include:

- the use of add, modify, and delete functions to implement changes to data;
- the procedures to prevent programs running in the wrong order or running after failure of prior processing;
- the use of appropriate programs to recover from failures to ensure the correct processing of data;
- protection against attacks.

The integrity of electronic mail communication can be ensured by using the encryption and signing functionality based on PGP-Keys or S/MIME certificates.

Output validation may include:

- plausibility checks to test whether the output data is reasonable;
- reconciliation control counts to ensure processing of all data;
- providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision, and classification of the information;
- procedures for responding to output validation tests;
- defining the responsibilities of all personnel involved in the data output process;
- creating a log of activities in the data output validation process.

9.6.4 Cryptographic controls

Objective
Confidentiality, authenticity, and integrity of information shall be protected by cryptographic means. Cryptographic keys shall be managed and protected against disclosure, modification, loss, and destruction.

Policies
A policy on the use of cryptographic controls for protecting information shall be developed, implemented and maintained.

Security Measures
Cryptographic controls should be used to achieve different security objectives, including:

- confidentiality: using encryption of information to protect sensitive, critical, or very critical information, either stored or transmitted;
- integrity/authenticity: using digital signatures or message authentication codes to protect the authenticity and integrity of stored or transmitted sensitive or critical information;
- non-repudiation: using cryptographic techniques to obtain proof of the occurrence or non-occurrence of an event or action.

Encryption keys shall be based on open algorithms and be derived from a random with sufficient entropy to prevent brute force attacks.

Key management shall be in place to support the developer's use of cryptographic techniques.

All cryptographic keys shall be protected against modification, loss, and destruction. In addition, secret and private keys need protection against unauthorized disclosure. Equipment used to generate, store and archive keys shall be physically protected.

Examples
A key management processes typically includes:

- generating keys
- generating and obtaining public key certificates;
- distributing keys to intended users, including how keys are activated when received;
- storing keys, including how authorized users obtain access to keys;
- changing or updating keys including rules on when keys should be changed and how this will be done;
- dealing with compromised keys;
- revoking keys;
- recovering keys;
- archiving keys, e.g. for information archived or backed up;
- destroying keys;
- logging and auditing of key management related activities.

9.6.5 Security of system files

Objective
Operating systems and applications shall be secured and protected against unintentional alteration. Access to program source code shall be restricted.

Policies
Administrator rights shall be regulated in a policy describing how they are granted, monitored, and revoked.

Access for vendors and service partners shall be detailed in a policy.

A policy shall define installation of software on operational systems, including developers approach to updates and patches.

A policy shall describe generation and utilization of test data, where applicable.

Security Measures
Control of operational software

To minimize the risk of corruption to operational systems, the following topics should be considered to control changes:

- updating of the operational software, applications, and program libraries is performed by IT administrators upon IT internal processes.
- Users are not allowed to install software which is not approved by the developer.
- The process to add new software should include defined testing and release scenarios.
- Patches and updates should be provided in a timely manner. In production environments service windows should be defined to allow updates to highly available systems.

Any decision to upgrade to a new release should take into account the business requirements for the change, and the security of the release, i.e. the introduction of new security functionality or the number and severity of security problems affecting this version.

Physical or logical access for suppliers should only be granted for support purposes for the time necessary. The supplier's activities shall be monitored.

Computer software may rely on externally supplied software and modules, which should be monitored and controlled to avoid unauthorized changes which could introduce security weaknesses.

Protection of system test data
Test data shall be carefully selected, protected and controlled.

The use of operational databases containing sensitive information for testing purposes should be avoided. If sensitive information systems have to be used for testing purposes, all sensitive details and content should be removed or modified beyond recognition before use.

Access control to program source code
Access to program source code and associated items (such as development tools, test cases, etc.) should be strictly controlled in order to maintain integrity of the TOE.

The TOE and its parts shall be controlled by a CM system.

9.6.6 Security in development and support processes

Objective
Security of applications, tools, and information shall be maintained.

Security applications and applications with impact on the TOE shall be controlled.

Applications developed by or on behalf of developer shall be fully compliant with specification and must not introduce any security weakness.

Policies
The release process for development applications and tools shall be documented.

A change management policy shall be defined and effective.

Perpetuation of confidentiality across applications, tools, and networks shall be documented.

Security Measures
Change control procedures

Change control procedures shall be documented and enforced in order to minimize the corruption of information systems. Introduction of new systems and major changes to existing systems should follow a formal process of documentation, specification, testing, quality control, and managed implementation.

This process should include a risk assessment, analysis of the impact of changes, and specification of security controls needed. This process should also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained.

Technical review of applications after operating system changes
When operating systems or applications are changed, critical applications shall be monitored to ensure there is no adverse impact on security.

Responsibility for monitoring vulnerabilities and vendors releases of patches and fixes shall be assigned.

Restrictions on changes to software packages
Modifications to software packages with impact on the TOE and its parts (e.g. development tools, test cases) should be discouraged, limited to necessary changes, and all changes shall be strictly controlled.

As far as possible, and practicable, vendor-supplied software packages should be used without modification. If changes are necessary the original software should be retained and the changes applied to a clearly identified copy. A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software. All changes should be fully tested and documented, so that they can be reapplied if necessary to future software upgrades.

Information leakage
Where confidentiality is required opportunities for information leakage shall be prevented.

Outsourced software development (informative)

Developer should monitor and control outsourced software development.

Where software development is outsourced, the following points should be considered:

- licensing arrangements, code ownership, and intellectual property rights;
- escrow arrangements in the event of failure of the third party;
- contractual requirements for quality and security functionality of code;
- testing before installation to detect malicious code.

Examples
In a typical high security area the outbound data transmission is restricted to defined people, and logged. Where utilization of mobile data media, e.g. USB-Devices, is inevitable, it is restricted to persons with approved privileges, e.g. by means of port protector tools. Data is encrypted before leaving a secure network.

Secure development lifecycle procedures are widely used to control software development.

9.6.7 Technical Vulnerability Management (informative)

Objective
Risks resulting from exploitation of published technical vulnerabilities should be mitigated.

Policies
A policy should detail developer’s approach to updating and patching.

Security Measures
There are two main different threads: published technical vulnerabilities of purchased software and systems, and self developed systems with improper implementation of security measures.

Timely information about technical vulnerabilities of information systems being used should be obtained, the developer's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

Where confidentiality and/or integrity are requirements, security should be integral part of software and system development projects.

9.7 Information security incident management

9.7.1 Overall Objective

Effective management of information security incidents shall ensure an appropriate level of security.

9.7.2 Reporting information security events and weaknesses

Objective
All security related incidents and weaknesses shall be reported to the Security Manager in a manner allowing timely corrective action to be taken.

Policies
The developer shall have a security incident management policy providing suitable feedback processes to ensure timely communication of security incidents. In particular, minimum criteria for reporting an event should be defined.

Security Measures
Information security events shall be reported through appropriate management channels as quickly as possible

All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.

The report shall be addressed to the Security Manager, where possible with evidence. Depending on the context it may be necessary to react immediately or wait Security Manager decision for action.

9.7.3 Management of information security incidents and improvements

Objective
Information security incidents shall effectively be resolved and improvements shall be implemented in a timely manner.

Policies
Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to security incidents.

Security Measures
All security incidents shall be reported immediately to the Security Manager. Beside immediate containment all responses to security incidents shall be agreed upon with the Security Manager.

Every security incident should be documented in an access controlled, secured environment. Records should be maintained.

Information security incidents should be analyzed, corrective and preventive actions derived and results reported in the regular security report.

Examples
The respective policy describes the expected types of incidents, corresponding containment, and mitigation.

Types, volumes, and costs of information security incidents are quantified and monitored.

Where a follow-up action against a person or organization after an security incident involves legal action (either civil or criminal), evidence is collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdictions (e.g. code of criminal procedure, privacy legislation, workers council involvement).

9.8 Business continuity management

9.8.1 Overall objective

Business continuity management shall ensure uninterrupted availability of processes, systems, and tools necessary to maintain the required level of security and/or integrity of the TOE and its part.

9.8.2 Security aspects of business continuity management

Objective
Integrity and - where required - confidentiality of the TOE and its parts shall be maintained in case of incidents, accidents, and crisis situations.

Policies
A managed process shall be developed and maintained for business continuity throughout the organization that addresses the security requirements.

Business continuity plans shall be documented and deployed in order to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, security relevant processes.

Security Measures
The developer is responsible for business continuity planning in his respective business within the framework of his entrepreneurial responsibility. All existing design, production, logistics and supply chain systems, structures and processes shall plan for sufficient contingency to appropriately mitigate the effects of disasters, business interruptions and/or risks as identified in accordance with risk assessment procedures.

Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for the TOE or its parts.

In terms of IT and information security the process should address network protection, computer centers incl. hardware, access control systems, and monitoring and alarm systems.

Where confidentiality is required, attention shall be put on the protection of the TOE in case of an incident. This should include, but is not limited to:

- Automated shut down of IT systems;
- Automatically closing emergency exits;
- Deployment of additional security staff.

A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address security requirements, and to identify priorities for testing and maintenance.

Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective.

9.9 Compliance (informative)

Objective
Breaches of any statutory, regulatory or contractual obligations related to the TOE should be prevented.

Policies
A policy should detail developers approach to the identification of relevant legislation, statutory, regulatory and contractual requirements, third party intellectual property rights, and other applicable regulations.

Security Measures
It is necessary to identify relevant legislation, statutory, regulatory and contractual requirements, third party intellectual property rights, and other applicable regulations.

Developer should assign this task to appropriately trained employees or use external service providers.

29. ANNEX 3: APPLICATION OF CC TO INTEGRATED CIRCUITS

PURPOSE

This annex presents a detailed application of all security assurance classes to the specific type of products, i.e. Integrated circuits.

PARTICULAR STATUS

None.

CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE

Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS.

1 INTRODUCTION

Complex microchips, which are able to process information, unfortunately introduce risks and dangers as well as huge advantages. Dependence on trouble-free functioning, as well as on the effectiveness of the protection measures, which have been carried out at the system and chip levels, has grown a great deal.

One must therefore be aware of the increased opportunities to test important information systems, including hardware against accepted criteria, in order to make the assurance of the security measures more transparent to the manufacturer, operator and user.

This annex shall serve as a handbook for the application of CC to hardware components in respect of integrated circuits. This document will be of particular interest to manufacturers, evaluators and certifiers.

1.1 Objective

The security properties of both hardware and software products can be certified in accordance with the CC. To have a common understanding and to ensure that CC is used for hardware integrated circuits in a manner consistent with today’s state of the art hardware evaluations, the following chapters provide guidance on the individual aspects of the CC assurance work packages in addition to the Common Evaluation Methodology [CEM].

This guidance is applicable to the hardware of single ICs. It covers assurance levels as defined in CC, i.e. EAL1 to EAL5. These are the evaluation levels used for hardware integrated circuits today. This guidance addresses mainly current Security IC level EAL4 to EAL5 and augmentations like AVA_VAN.5.

1.2 Glossary

Following terms are defined by CC Part 1.

BiCMOS	Bipolar Complementary Metal Oxide Semiconductor, specific semiconductor technology
CAD	Computer Aided Design
CMOS	Complementary Metal Oxide Semiconductor, specific semiconductor technology
Die	individual IC on a wafer (plural ”dice”)
EPROM	Erasable Programmable Read Only Memory
E2PROM	Electrically Erasable Programmable Read Only Memory
HDL	Hardware Description Language
HW	Hardware
IC	Integrated Circuit, integrated electronic circuits in a microchip
SW	Software
Wafer	Silicon slice for chip production

2 ASSURANCE REQUIREMENTS FOR INTEGRATED CIRCUITS

2.1 Introduction

In applying CC to hardware components, two types of Target of Evaluation (TOE) may be considered:

- a TOE produced from a series of discrete parts on a printed circuit board or as a hybrid through different or several dice on one carrier;
- a TOE produced as an individual integrated circuit (IC).

The following guidance concerning the CC assurance aspects for a TOE is applicable to the hardware of single ICs.

In general, logical functionality in an IC can be implemented in simple PLD structures (Programmable Logic Device), FPGA structures (Field Programmable Gate Array), as an ASIC (Application Specific Integrated Circuit), or as well as a customer IC.

In respect of security applications, intelligent memory ICs with a hard-wired security logic (e.g. public transport cards, building access control or micro-controller based ICs in an ASIC design (e.g. electronic purse ICs) are used mainly for the elementary core components of security functionality.

Contemporary memory in ICs is based on EPROM, E2PROM or flash cells. This enables the non-volatile storage of data. Security logic can be utilised to implement identification and authentication, access control and internal IC sequence controls.

Micro-controller-based ICs offer the possibility of carrying out independently complex processes controlled by an IC operating system. Items, which also belong to the aforementioned functionality, comprise accountability functions and services such as encryption, random number generation and digital signature, functionality that is implemented in hardware as well as software.

The mechanisms for the protection of software and operational data in various memories and the internal sequences are realised through the hardware of an IC (e.g. by means of certain technical measures and technological features) in order to support logical functionality.

An operating system of a micro-controller IC is contained (placed) in a ROM and/or an E2PROM memory, and is protected from disclosure and modification during the operational phase by the technical or technological properties of the hardware. While technological properties are inherent in a TOE, technical properties depend on the design of the TOE.

2.2 CC Approach for Evaluation

The CC prescribes a variety of assurance activities, such as TOE specific as design analysis, guidance documentation, vulnerability analysis, penetration testing, on the one hand and the examination of development and production environment on the other hand. Whilst there are differences in terminology used, fundamentally the two sets of criteria are very similar in terms of specifying assurance requirements, and in their underlying philosophy.

A unique feature of the CC is the introduction of the Protection Profile concept. A Protection Profile can be characterized as a generic Security Target for a particular class of TOE (e.g. Security ICs, as in the case of [BSI-CC-PP-0084-2014][34], which defines a recognized standard to which conformance may be claimed. Whilst it is not mandatory to claim conformance to a Protection Profile, the availability of such standards provides the potential to reuse evaluated material in a Security Target, thereby considerably easing the process of producing this particular evaluation deliverable for the developer. For the user, conformance to one PP by several STs (i.e. by different products) allows comparison of these products on an equal basis. Especially in the case where there is a single, well-established Protection Profile for that domain, this is a strong mechanism that gives the user more choice and better cost-efficiency.

A Protection Profile (PP) may be defined, evaluated and certified in advance of a real TOE Evaluation and can be referenced within the Security Target of the real TOE Evaluation. There are two types of conformance: demonstrable and strict. In the demonstrable case, the security functional requirements (SFRs) of the Security Target are argued to be similar to the ones in the PP. In the case of strict conformance, the ST is conformant to a PP only if it is compliant with all parts of the PP. The PP referenced sets the level of conformance required. In the Security IC domain, strict conformance is most common.

The following chapters provide guidance for hardware TOEs that have to be evaluated under Common Criteria (CC).

[34] Security IC Platform Protection Profile with Augmentation Packages.

The evaluation of the IC comprises the following activities:

- Security Target,
- Development,
- Tests,
- Guidance including operation
- Life-cycle support, including configuration management and delivery
- Vulnerability assessment.

The above mentioned activities correspond to certain assurance classes defined in the CC Part 3. The following table shows the Assurance Class / Assurance family breakdown and mapping.

Table 1 - Assurance family breakdown and mapping

Assurance Class	Assurance Family	Abbreviated Name
Class APE: Protection Profile Evaluation		APE[35]
Class ASE: Security Target Evaluation		ASE[36]
Class ADV: Development	Security Architecture Functional specification TOE Design Implementation representation TSF internals Security policy modelling	ADV_ARC ADV_FSP ADV_TDS ADV_IMP ADV_INT ADV_SPM
Class ATE: Tests	Coverage Depth Functional tests Independent testing	ATE_COV ATE_DPT ATE_FUN ATE_IND
Class AGD: Guidance documents	Operational user guidance Preparative procedures	AGD_OPE AGD_PRE
Class ALC: Life cycle Support	CM capabilities CM scope Delivery Development security Flaw remediation Life-cycle definition Tools and techniques	ALC_CMC ALC_CMS ALC_DEL ALC_DVS ALC_FLR ALC_LCD ALC_TAT
Class AVA: Vulnerability assessment	Vulnerability analysis	AVA_VAN

CC assurance families are split up into certain hierarchical assurance components. These components are directed to predefined Evaluation Assurance Level (EAL) packages (EAL1 to EAL7). A combination of certain assurance components builds up one of the predefined EAL-packages as shown in CC Part 3, chapter 8.

To perform a TOE evaluation, an EAL-Package can be used as predefined by CC (Part 3 conformant). Besides this, augmentation or extension of an EAL package is possible (for details refer to CC, Part 1).

The following discussion gives guidance on how to use the assurance components of CC Part 3 assurance classes for hardware IC TOEs (e.g. a Security IC Platform).

It is recommended to use one of the predefined EAL-Packages for a TOE Evaluation. In most cases, for an evaluation of hardware IC (e.g. Security IC Platform) an augmentation of the selected EAL package is necessary to fulfil specific objectives (e.g. for a high-level vulnerability assessment). If so, all dependency requirements as outlined within CC Part 3 have to be fulfilled. The following discussion will refer to augmentation aspects within the relevant paragraphs.

[35] The assurance class APE is split into several families (see CC Part 3).
[36] The assurance class ASE is split into several families (see CC Part 3).

2.3 CC Protection Profile (Class APE)

Unlike a ST, which describes implementation oriented security; a PP describes abstract security requirements. For instance, the requirement for a random number generator (RNG) with an un-specified quality could be expressed in a PP, and a compliant ST could then state to what quality level the particular TOE provides random numbers.

The majority of guidance applicable to a ST applies equally well to a PP (see the next chapter) for example, definition of scope and boundary of TOE, environmental assumptions, threats, security objectives.

The reference PP related to IC and conformant to CC is [BSI-CC-PP-0084-2014]. It has been developed by a community of semi-conductor manufacturers and takes advantage of wide experience in Smartcard security. For more PPs refer to the website on European cybersecurity certification schemes maintained by ENISA.

2.4 CC Security Target (Class ASE)

2.4.1 Objectives

The Security Target (ST) for a TOE is the basis for the evaluation and shall be agreed between developer and evaluator. The audience for the ST is not confined to those responsible for the production of the TOE and its evaluation, but may also include those responsible for managing, marketing, purchasing, installing, configuring, operating and using the TOE.

Annex A of CC Part 1 describes in details the content and presentation requirements of the ST.

A Security Target comprises the following:

- a precise description of the security problem solved by the TOE and its environment in terms of threats, any assumptions, organisational security policies and intended use;
- a description of the security objectives for the TOE and for the environment in order to determine whether the security objectives counter the identified threats, achieve the identified organisational security policies and adhere to the stated assumptions.
- Protection Profile claims if any exists;
- a description of the security functional requirements and security assurance requirements of the TOE;
- a summary specification of how the TOE implements the security functional requirements;
- a rationale giving justification for transformation of the security problem to the security objectives to the security requirements.

Following sections provide observations concerning individual requirements.

2.4.2 Input

The developer shall provide the document ”Security Target”.

2.4.3 Requirements

TOE description

The Security Target shall include a precise description of the Target of Evaluation (TOE) in terms of hardware, software and firmware components. Reference to technological parameters is also important. The TOE description shall explicitly state the nature of any dedicated test software (either embedded software or software outside the integrated circuit).

The general security characteristics of the hardware shall also be described. A reference to the hardware datasheet would be appreciable. All possible configurations or intended use of the chip shall be identified.

The TOE needs to be clearly identified and separated from its technical and operational environment. The ST shall uniquely reference the TOE.

Since the hardware parts of an IC are both physically and functionally difficult to separate from one another without additional information, it is not possible to exclude parts of the hardware from the TOE; it is therefore sensible to define the whole of the IC hardware as the TOE. In the case of certain parts of the IC being outside the TOE, a clear, logical and physical interface must exist. The inclusion of strongly hardware-oriented software/firmware in the TOE is appropriate. It would be sensible to look at an IC in its entirety and not only at the hardware or only at the software.

Security Environment
The security environment of the TOE comprises the operational environment after delivery as well as the technical environment in the different phases of the lifecycle of the TOE.

Therefore, a precise description of the TOE lifecycle is required or should be referenced. The boundaries of the TOE in terms of lifecycle shall be defined.

The Security Target shall explicitly state which phases of the life cycle are under the scope of the evaluation and which phases are excluded; the phases where the TOE is being developed and manufactured shall always be within evaluation scope.

In contrast with purely software TOEs, as in the cases noted here, this determination is only possible with precise knowledge of the manufacturing process. However, this statement also has a direct influence on the threat and attack scenarios in the operation of the TOE, which could be adopted in the context of the evaluation of the TOE. In the case of an IC TOE, the cut-off for evaluation could be after testing the IC as a die (at the earliest), or upon completion of packaging and associated testing. Optionally, the Security Target may include further phases of the IC such as micromodules assembly, pre-personalisation and personalisation phases.

The CC explicitly require that threats be characterized in terms of an identified threat agent, the asset at risk, and the attack. Thus it is necessary to define and enumerate all subjects in terms of roles and the assets for which specific protection either by the TOE or its environment is required and with reference to the lifecycle phases of the TOE.

Any assumptions placed on the environment, with which the TOE or its environment must comply, have to be identified.

Assumptions relating to the operation of the software, which is not part of the TOE are essential. These may include:

- integrity protection software, e.g. for responding to sensors, or to watchdog timer interrupts;
- implementation of algorithms that are DPA-resistant;
- fault-handling software (e.g. protecting against inducing faults to enable a differential fault analysis attack on cryptographic keys).

Regarding the operational phase of the TOE, any assumption on the security aspects of the environment in which the TOE will be used or is intended to be used shall be described. Generally for a Security IC, no specific assumption for the TOE and its environment during the end-user phase (operational environment) has to be defined since this environment is a public one. However, if the TOE comprises only IC-hardware, there may be important security assumptions for the usage-phase of the TOE.

With reference to the lifecycle phases which are beyond the scope of the evaluation, there should be information about who is able to use the TOE after delivery and in what operational modes it is possible to use it. In this context, the actions of all personnel who come into contact with the TOE after delivery need to be examined. Therefore, specific assumptions about the behaviour of such personnel need to be defined and an identification of operational roles involved is necessary. Note: hardware may add a variety of roles that are IC-specific, e.g. there may be different approaches to personalization and enablement; such hardware-specific roles may need to be documented outside of the ST.

As an example for specific assets for a Security IC this may include:

- IC specific data including personalisation data and cryptographic keys,
- smartcard embedded software,
- IC dedicated software,
- Specific Application data like keys, authentication data or access control information.

A distinction might be useful between primary assets - such as the data stored and operated by the Security IC Embedded Software, the Security IC Embedded Software itself when stored and in operation, and the security services provided by the TOE for the Security IC Embedded Software - and secondary assets which, if compromised, could be exploited to compromise a primary asset. Secondary assets do not have any intrinsic value as such, but instead derive value from the primary assets. This distinction would allow a separation of high and low-level assets, which in turn will help to structure the statement of threats and thereby lead to a better understanding of the security objectives and security requirements to be met by the IC.

However, the CC do not mandate that low-level or secondary assets are identified in order to drive the selection of security objectives and requirements. For example, integrity protection SFRs can be included simply to help achieve a security objective for protection of a high-level or primary asset - with the security requirements rationale explaining the purpose of such SFRs.

Assumed threats to the assets shall be described. The CC require that threats defined in the ST, are not directed at the identified security objectives, but rather are addressed by the security objectives. It should also be noted that the CC explicitly require that threats be characterized in terms of an identified threat agent, the asset at risk, and the attack (describing such aspects as attack methods employed, vulnerabilities exploited, and opportunity).

It shall be a description in terms of damages to the assets rather than attack paths, which could not be completed in the ST. The threats could be described in terms of:

- unauthorized disclosure of assets;
- unauthorized use of assets;
- unauthorized modification of assets.

To be able to understand the threats defined for the environment of the TOE in certain phases of the lifecycle, the TOE's development and production environment shall be described.

Beside logical functionalities, technical and technological properties can be attacked during the operational phase of the TOE, too. The corresponding threats to the defined assets can therefore be formulated (e.g. selection of objects also by means of physical attacks, operation of the TOE outside specific parameters, such as voltage, frequency and temperature).

With respect to determining specific threats, it should be noted that attacks on ICs during production processes, and in particular during test phases, are possible and shall be considered for the relevant life-cycle phases within the relevant assurance class ALC. They may result in vulnerabilities in the development of the TOE identified by the evaluator during the conduct of evaluation activities for class ALC.

Specifications of organizational security policies depend essentially on the applications in which the TOE is incorporated. Generally speaking, for a pure hardware Security IC evaluation, no specific organizational security policy has to be defined.

Security Objectives

The CC require that security objectives be specified within the ST for both the TOE and the environment that are necessary to counter the threats and uphold the identified assumptions and organizational security policies.

The objectives shall be clearly stated to permit a clear mapping back to the relevant threats. They could be derived from the following:

- resistance against physical manipulation;
- resistance against physical probing;
- protection from information leakage (naturally occurring and attacker-induced);
- protection of test functionality;
- storage of data by test personnel;
- providing random numbers.

Technical and technological properties of the IC beyond the objectives, i.e. those providing self protection, will be addressed in the ADV_ARC evaluation activity. The ST author can choose to highlight these properties to users in the TOE Summary Specification (as part of ASE_TSS.2).

Additionally, there may be a need for specific security objectives on the environment to ensure that assumptions concerning dependencies on software are upheld.

Security objectives for the environment within certain lifecycle phases might be satisfied by measures for the environment of the TOE evaluated by the assurance requirements for the development process of the TOE. (e.g. development security).

Security requirements

Security requirements shall be defined within the ST using the functional and assurance components specified in the CC Parts 2 and 3. In some cases, if predefined functional components of the CC Part 2 are not applicable, new IC-specific components might be defined within a ST.

It is required that the security functional requirements (SFR) and assurance requirements (SAR) on the TOE are needed to meet the identified security objectives for the TOE.

SAR
The required level of attack potential for the vulnerability analysis is expressed in CC requirements by selection of a certain AVA_VAN assurance component. This component defines the baseline for the protection of the TOE in terms of attack potential against which the vulnerability analysis of the TOE will be judged.

The evaluators' independent vulnerability analysis builds on information gained from all other evaluation activities and goes beyond the security architecture description (often seen as "the developer's vulnerability analysis"). The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a basic (for AVA_VAN.1 and AVA_VAN.2), enhanced-basic (for AVA_VAN.3), moderate (for AVA_VAN.4) or high (for AVA_VAN.5) attack potential.

By way of example, to ensure resistance against high attack potential for vulnerability analysis at EAL4, the AVA-class has to be augmented with AVA_VAN.5. Additionally, the components which AVA_VAN.5 depends on have to be required within the SAR. For more information on attack potential refer to Annex 7, APPLICATION OF ATTACK POTENTIAL TO SMARTCARDS AND SIMILAR DEVICES.

SFR
Some guidance on the use of such components in a PP or ST for an IC might be helpful, although there are now a number of PPs in existence for ICs which can be usefully referenced (indeed, a need to comply with such PPs may pre-determine which functional components must be used in the ST).

Possible CC Part 2 Security Functional Requirements (SFRs) for an IC comprise for example components from the following classes: FIA, FMT, FCS, FDP, and FPT.

It is important that the selected functional components be tailored to the extent necessary to demonstrate that the TOE security objectives are met. This applies to both PPs and STs (but especially the former, where operations on functional components can be left uncompleted, thus resulting in SFRs, which are too generic).

A further issue is the CC requirement that SFRs are actually testable. For guidelines on testing refer to ATE below.

The FPT_PHP components are used to express requirements for protection of the TOE from physical tampering attacks and require the TOE to implement functions to respond to these attacks - whether by:

- providing the capability to detect an attack (FPT_PHP.1); or
- detecting and providing notification of an attack (FPT_PHP.2); or
- responding automatically to resist an attack (FPT_PHP.3).

The selection of these components might be adapted to the situation in place. For example, responding automatically to resist an attack (FPT_PHP.3) may be refined as assuming that there might be an attack at any time and therefore providing countermeasures at any time because the TOE´s technical properties may not be able to detect the attack but are activated in place permanently. For example, permanent protection against Differential Power Analysis is required, ensuring that the SFR could not be violated or bypassed at any time.

In the evaluation of a composite TOE (IC hardware plus software: operating system, application software and IC dedicated software) it may be applicable to select functional components for an information flow control policy through the use of functional components from the FDP_IFC and FDP_IFF families. These components apply to certain parts of the software which are part of the TOE (for example such requirements are placed on the OS and hence on the integrated platform comprising IC and OS; in [BSI-CC-PP-0084-2014] such components are applied to IC dedicated software).

A ST or PP may modify selected CC Part 2 components to be more meaningful to smartcards, (however, it should be noted that modified requirements like this need to be proven in practice) such as:

- a deviation from audit data generation component, FAU_GEN.1 to exclude the requirement for date and time in the audit record. However, this requirement is only achievable if an externally trusted time source exists and trust can be preserved in the record;
- a refinement of FPT_TST.1, self-processing, to include card blocking functions.

Operations on requirements
The Security Target shall explicitly perform all the operations (assignment, iteration, selection, and refinement) of the security requirements. These operations may concern both functional security requirements as well as assurance security requirements. As a minimum, all the operations of assignment and selection of functional security requirements shall be performed.

For each selection, the Security Target author shall select the appropriate item in the selection list. For each assignment, the Security Target author shall specify the appropriate item. Any guidance could be found in the annexes of the CC Part 2.

For ICs, it is important that security aspects of design and implementation, which are not necessarily functional in nature, be addressed by the evaluation.

TOE summary specification (TSS)

The TOE summary specification provides a high-level description how the TOE implements the functional requirements (SFR) as defined in the ST. The ST author can choose to highlight technical and technological properties of the IC to users in the TOE Summary Specification (as part of ASE_TSS.2).

PP claims

The Security Target shall explicitly claim compliance with any Protection Profile if applicable. In this case the ST must claim the conformity explicitly.

[BSI-CC-PP-0084-2014] which has been developed by a community of semi-conductor manufacturers could be referenced[37] in the Security Target.

It shall be noted that claims of partial compliance to a PP is not permissible under the CC. PP compliance can be demonstrable or strict, as defined in the Protection Profile referenced. In the Security IC domain, strict PP compliance is preferred.

In case of any PP compliance, the Security Target does not need to repeat statements of security requirements included in the PP that are unmodified for the Security Target. Nevertheless, it could be easier to have an independent document.

If, however, the PP includes uncompleted operations, which is the case for [BSI-CC-PP-0084-2014], completing these operations is the responsibility of the Security Target author.

Rationale

The security target is fundamental to set up an effectiveness view since it lists the intended use of the IC, the operational environment, the assumed threats, objectives, functional and assurance requirements and the TOE summary specification as discussed above.

The CC require a rationale, which demonstrates that a TOE conformant with the ST will effectively address all relevant aspects of the 'security problem' defined by the Statement of Security problem definition. The ST rationale presents the analysis in a step-wise manner:

- firstly, the security objectives for the TOE and its environment must be shown to be suitable to counter the identified threats (transposed by certain attack scenarios) and uphold all identified policy needs and assumptions. If applicable, scenarios of physical attacks on the hardware can be of significance. Assumptions made relating to the software operation are essential;
- secondly, the security requirements must be shown to be suitable to satisfy the TOE security objectives, and be mutually supportive and provide an integrated and effective whole (binding). Therefore, the analysis should consider combinations of SFR where some of them may be logical and others technological and technical requirements. The analysis should also consider relations between assurance requirements and objectives for the operational environment of certain phases of the lifecycle like composite product integration and personalization phases.

Binding of hardware- and firmware-functionalities is to be taken into consideration, depending on the scope of the TOE. For an IC, the Security Target should describe the assumptions made relating to the software operation.

Detailed aspects addressing the issue of indirect attacks against the IC (e.g. bypassing or contradicting the TSF) should be part of the vulnerability assessment (see class AVA). The developer supports this with his view on how indirect attacks in the form of bypass or tampering are countered (in the security architecture description, evaluated in ADV_ARC).

In the evaluation of a composite TOE, the analysis should discuss the interrelationships between the software and hardware parts of the TOE to demonstrate that they are mutually supportive in helping to meet the Security Target for

[37] For a list of applicable PPs refer to the website on European cybersecurity certification schemes maintained by ENISA.

the composite TOE. This will not only involve discussion of dependencies of the IC on the software such as those listed above, but also the software dependencies on the hardware, including tamper-resistance aspects.

Analysis is mostly done by providing mappings in combination with informal arguments of the mapped items and explanations on relations between certain items.

2.5 Development (Class Adv)

The assurance class ADV defines requirements for the stepwise refinement of the TOE Security Functionality (TSF) from the TOE security functional requirements (SFR) in the ST down to the actual implementation, and defines requirements for the description of architectural oriented features and internal structure of the TOE (ADV_ARC, ADV_INT). Each of the resulting TSF representations provides information to help the evaluator determine whether the functional requirements of the TOE have been met.

The technical description of the TOE is always accompanied by mapping the higher-level to the lower-level of the TOE representations.

2.5.1 Architecture (ADV_ARC)

2.5.1.1 Objectives

CC Part 3 introduces the security assurance family Security Architecture (ADV_ARC). Its objective is described as follows:

“The objective of this family is for the developer to provide a description of the security architecture of the TSF. This will allow analysis of the information that, when coupled with the other evidence presented for the TSF, will confirm the TSF achieves the desired properties. The security architecture descriptions support the implicit claim that security analysis of the TOE can be achieved by examining the TSF; without a sound architecture, the entire TOE functionality would have to be examined.”

The family ADV_ARC requires the TOE security architecture to describe the self-protection, domain separation and non-bypassability principles. The Security Architecture shall also describe the secure TOE security functionality (TSF) initialisation.

2.5.1.2 Input

The security architecture description shall be made available at all EALs from EAL2. The developer shall provide a security architecture description of the TSF at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

The security architecture description shall demonstrate the effectiveness of self-protection and non-bypassability.

2.5.1.3 Requirements

Non-bypassability is a property that the security functionality as specified by the SFRs is always invoked and cannot be circumvented when appropriate for that specific mechanism (cf. to Annex A of CC part 3, paragraph 517). CC Part 3, A.1.2.3 discusses the bypassability of the SFR-enforcement through different interfaces and the information provided in the functional specification (ADV_FSP) and TOE design (ADV_TDS) about the operations and information available trough these interfaces. This includes all logical and physical programming and communication interfaces of the IC as well as the surface of the IC.

Self-protection refers to the ability of the TSF to protect itself from manipulation from external entities that may result in changes to the TSF, so that it no longer fulfil the SFRs. Self-protection of the TSF will be achieved by:

- self-protection of TSF mechanisms: the ability of a TSF mechanism to protect themselves against direct attacks to interfere, to manipulate or to disable this mechanism;
- binding of TSF mechanisms: the ability of the TSF mechanisms to work together in a way that is mutually supportive and provides an integrated and effective whole.

Example of self-protection of a TSF mechanism is the protection against physical probing of a security IC to manipulate or to disable TSF features. In some cases the physical protection mechanism must resist such attacks independent on any other TSF mechanism. In other cases the physical protection mechanism detects such attacks and the operating system reacts on it entering a secure state.

An example of binding of TSF mechanisms in case of smart cards is the combination of hardware and software TSF mechanisms:

- to ensure the stable correct execution of the embedded software under specified operational conditions;
- to detect errors of the execution caused by perturbation;
- to enter a secure state if detected errors can not be automatically corrected.

The security architecture description shall describe how the TSF initialization process is secure (cf. ADV_ARC.1.3C). The information provided in the security architecture description relating to TSF initialisation is directed at the TOE components that are involved in bringing the TSF from the “down” state (e.g. power-off) into an initial secure state (i.e. when all parts of the TSF are operational) (cf. CEM paragraph 529). The TSF may have parts providing their security function when the TOE is not running. E.g. the physical protection of a security integrated circuit shall resist tampering attacks according to FPT_PHP.3 even if power is off. Other parts of the TSF may be activated during start-up of the TOE before or at the same time when the relevant TOE functionality is activated. E.g. sensors shall control the environmental conditions for the normal secure operation of a security IC at time the operating system of the smart card starts-up. The operating system shall check the integrity of stored TSF data before relying on it. For security IC the secure initialisation process of the TSF covers power-on start-up, entering and wake-up from power save modes or any kind of reset.

Domain separation is a property whereby the TSF creates separate security domains on its own and for each untrusted active entity to operate on its resources, and then keeps those domains separated from one another so that no entity can run in the domain of any other (cf. CC Part 3, paragraph 515, 524 and 578). Security domains refer to environments supplied by the TSF for use by potentially-harmful entities (cf. CEM, paragraph 527). The environment provided by the TSF of the IC to an entity at the programming interface may comprise resources like

- input and output ports / interfaces to interact with external entities (users) or processes (subjects) of the IC dedicated or embedded software;
- address space to access operational memory and functional registers;
- commands of CPU or cryptographic coprocessors available for execution by an entity;
- services provided by the TSF like random number generation.

The TSF may use specific resources for their own security domain only like e.g. sensors for environmental failure protection being outside control of the embedded software. The TSF may share resources with other entities like e.g. random number generator used by the TSF for randomization of cryptographic coprocessor computation and used by the embedded software for key generation. The TSF may control access to resources by entities of different security domains but not used by its own like privileged CPU commands. The TSF may provide security capabilities for the embedded software to enforce their domain separation e.g. a memory management unit.

2.5.2 Functional specification (ADV_FSP)

2.5.2.1 Objectives

The functional specification describes the TSF interfaces (TSFI), and must be a complete and accurate instantiation of the TOE security functional requirements as defined in the ST.

The goal of the ADV_FSP family is the description and analysis of the external interface to the TOE. Users of the TOE are expected to interact with the TSF through this interface. The TSFI consist of all means for users to invoke a service from the TSF (by supplying data, signals, energy or physical effects that are processed by the TSF) and the corresponding responses to those service invocations. These service invocations and responses are the means of crossing the TSF boundary (cf. [CC] part 3, section A.2.1). All interfaces crossing the border of the TSF including interfaces to the non-TSF subsystems of the TOE are considered as TSFI. The TSFI description provides necessary information to conduct testing.

The components ADV_FSP.2 and higher describes in increasing levels of details all TSFI. At lower-level components, the developers may focus their documentation (and evaluators focus their analysis) on the more security-relevant aspects of the TOE by characterization of the TSFI as SFR-enforcing, SFR-relevant and SFR-non-interfering. The components ADV_FSP.4 and higher typically used for security IC describe all interfaces on the same level of details and allow for deeper analysis that the interfaces do not provide functions in a way contradicting the SFR defined in the ST.

2.5.2.2 Input

Regardless of the EAL level, the developer shall provide the functional specification.

The external interfaces are usually described in the data sheet for the IC. The ISO standard (7816) is of relevance in most cases. In addition, the die description shall be given.

2.5.2.3 Requirements

The functional specification usually uses developers' terminology. The level of detail required for the specification has to be correlated to the coverage of functional tests (ATE_COV) and to the external interface description within the guidance documents (AGD_OPE / AGD_PRE).

Specification of functional details of the TOE security functions has to be provided within the Functional Specification. More detailed representation levels map these functional details to the defined subsystems or modules.

External interfaces of an security IC can be classified as :

- Program interfaces – the logical interface to the software/firmware which is stored on the IC and is not part of the TOE, but which runs on the IC hardware under consideration (e.g. the triggering of an interrupt via hardware, test software interfaces).
- Communication interface – the logical interfaces (e.g. instruction set, special function register specification, memory map) and the physical interfaces of the IC (IC contacts with serial I/O and supply or contactless interface or both), which guarantee the connection to the outside world within the operational environment and the operating system / application programming environment.
- IC surface – an explicitly defined continuous perimeter that establishes the physical bounds of the TOE and contains all the hardware, software, and/or firmware components of the TOE. The IC surface shall be described and examined for physical protection (cf. SFR of the FPT_PHP family) and completeness of the logical and physical interface description, including areas of emanation and for irradiation.

For an IC, the physical entry or exit point of the TOE (ports) shall be described that provides access to the TOE for physical signals, represented by logical interfaces, including power supply. A port may provide more information than necessary for the TSFI. This additional information may bypass the security functionality intentionally provided through this interface (e.g. by a side channel). Simply observing external interfaces from the point of view of their logical behaviour is unlikely to be sufficient. Externally adjustable operational parameters and their limits should also be investigated because direct attacks or vulnerabilities may result. The functional specification shall trace the SFRs to TSFIs.

The IC Dedicated Test Software may be delivered as part of the TOE to support testing of the TOE during production and may not be usable after TOE Delivery. In this case the IC Dedicated Test Software (or parts of it) is seen only as a "test tool", which does not provide security functionality for the operational phase of the TOE. Their use shall be described in the guidance documentation for the tester but not necessarily in the Functional Specification. However, it must be verified that it cannot be abused after TOE Delivery: this is evaluated according to the CC Part 3 assurance family AVA_VAN.

The Functional Specification shall specify operating conditions of the security IC. These conditions include but are not limited to the frequency of the clock, the power supply, and the temperature. The security IC should respond to violation of operating condition threatening the correct execution of the embedded software by entering a secure state.

Semi-formal notation

At EAL5, the functional specification is required to be semiformal. Example given, the semi-formal description of the functional specification can take the form of

- tables, where every column is assigned to a specific bit of a specific register and informal text explains their effect;
- block diagrams, where all block diagrams used abbreviations and arrows to define the direction of the data flow;
- mathematic formula, e.g. Boolean logic expression describing the combination of signals or an inequation for the specification of the control of various thresholds;
- pseudocode used similar to the programming language and which does not include any unclear structures;
- assembler code describing program sequences to specify the behaviour and intended usage of specific components.

The informal documentation of the technical and technological properties, as well as their integration into the structure and the realization of SFR are necessary.

2.5.3 TOE design (ADV_TDS)

2.5.3.1 Objectives

The objective of these requirements is to provide both context for a description of the TSF, and a thorough description of the TSF. The design documentation shall provide sufficient information to determine the TSF boundary, and to describe how the TSF implements the SFR.

The design requirements are intended to provide information (commensurate with the given assurance level) so that a determination can be made that the security functional requirements are realised.

The TOE design provides a description of the TOE and TSF in terms of subsystems as major structural units with functional coherence, provides a description of the interaction of these structural units, and is a correct realisation of the functional specification.

The TOE design provides a description of the TSF in terms of modules as most specific description of functionality. The description of the modules shall provide sufficient details that the developer should be able to implement this part of the TOE described by the module with no further design decisions.

2.5.3.2 Input

TOE design information shall be made available at all EALs from EAL2.

2.5.3.3 Requirements

TOE vs. TSF

The TOE design describes the structure of the TOE in terms of subsystems and identifies the subsystems of the TSF. The TSF includes all parts of the TOE that contribute to the satisfaction of an SFR in the ST (in whole or in part) and the security architectural principles of TSF self-protection, domain isolation, non-bypassability and secure initialization (see ADV_ARC). Any part of the TOE not being part of the TSF must not prevent the TSF from satisfying the SFR in the ST.

If TOE subsystems are separated TSF subsystems, the justification about the clearness and effectiveness of the separation should be based on logical and physical dependencies. A maximal independence of subsystems within an IC TOE could be possible if there were no or only minimal physical overlaps and logical dependencies between the individual subsystems and the interfaces are clearly defined.

Basic structure of the TSF in terms of subsystems and modules:

The developer’s choice of subsystem definition and at level ADV_TDS.3 or higher the refinement into TSF modules within each subsystem are an important consideration in making the TOE design useful in understanding the TSF intended operation. The number of subsystems and modules within subsystems together with the description of their interaction, interfaces, and the purpose of the modules has to be appropriate and sufficient for the evaluator to gain the necessary level of understanding how the functionality of the TSF is provided.

If the IC design is managed through a classical process of hardware drawings, the development process depends essentially on the technologies used (specific method and tools) and can be described by refining design in terms of subsystems into a sufficient level of detail in terms of modules to implement the TOE. If the IC design is managed through a hardware description language (HDL), the decomposition is similar to those used in classical software development. The construction plans and functional descriptions, which result from the use of an HDL tool and a CAD tool, can be used directly during the construction of the TSF design, but needs only to be presented fully for ADV_TDS.4 or higher.

The TOE design provides a top level design specification in terms of subsystems of the TOE and the TSF. The complete data book comprising the complete description of the chip may be considered to support these requirements. A block diagram, which originates in the design and conception phase, as well as an informal description, can be an integral part of the TOE design description in terms of subsystems. Typically, the documentation needed for the subsystems may be described as a mapping of the major architectural components to the physical devices performing specific functions (e.g. CPU, RAM, ROM, Bus and I/O elements) and the interaction among the subsystems.

In many cases, components which represent the general structure of an IC TOE can be definite logical units; they are possibly even implemented as a physical unit on the IC. Examples comprise: memory, data/address bus–memory interface, arithmetic block, contact interface, watchdog timer, sensors with analysis logic, controls for the voltage supply, logic blocks for access controls or authentication for memory ICs with security logic, a micro controller block on micro controller ICs.

The TOE design at level ADV_TDS.3 or higher requires a refinement of the TSF subsystems into modules. Modules are described in detail in terms of the function they provide (the purpose); the interfaces they present; the return values from such interfaces; the interfaces (presented by other modules) they use; and a description of how they provide their functionality (one possible way to describe the functionality is an algorithmic description) (cf. CC Part 3, section A.4.2).

The form of description of the functionality and how the module provides them depends on the functionality. E.g. the TOE design may provide an algorithmic description for calculation of a cryptographic coprocessor as well as an informal description of the physical principle used for a sensor or a noise source of a physical random generator.

The design elements necessary for the construction of the TOE are:

- logical plans (which for example consist of analogue cells, standard cells, gates, transistors and diodes) or corresponding HDL-representations in order to realise individual functionality as well as security mechanisms;
- specification of the physical design which describes the requirements for the organisation of the physical components (e.g. module placement, layer order, routing specifications).

In the case of an IC, the actual logic and layout plans will have been derived from modules, whereby the separation of the modules has to fulfil the testing requirements. Interfaces between modules must be described especially carefully, since there are strong dependencies between them in an IC. Functionality, which runs in parallel, should be considered with the description of the interfaces. The timing of the module interfaces should be described if they are accessible from the outside (e.g. pads) for tests.

Since the security properties of an IC TOE can consist of logical functionality as well as technical and technological properties, it is necessary to document the general structure of the architectural components as well as to explain the technical and technological structure (general layout rules of the physical design: technology, number of layers, bus routing) because of their importance to the hardware security properties. A protective layer could, for example, be seen as a component of the general structure of the physical composition of the TOE.

The description of the TSF in terms of SFR-enforcing, SFR-supporting and SFR-Non-interfering subsystems and modules

The TOE design shall designate the TSF subsystems - and additionally at level ADV_TDS.3 and higher the modules - as SFR-enforcing, SFR-supporting and SFR-non-interfering. At lower-level components, developers may focus their documentation (and evaluators focus their analysis) on the more security-relevant aspects of the TOE, i.e. starting with SFR-enforcing and going further to SFR-supporting components up to SFR-non-interfering components. It should be noted that even when more or even complete information is required at higher level components, it is not required that all of this information be analyzed in the same level of detail. The focus should be in all cases on whether the necessary information has been provided and analyzed.

Mapping of the SFR to physical subsystems may not be easy to do (e.g. which subsystem really does process the security functions, the CPU or a CPU in conjunction with its associated memory and bus?). This is because within the IC itself there are strong dependencies between various physical components at the implementation level, which complicate an effective separation in the sense of the criteria. Consequently, it is mostly necessary and may be easier for some hardware TOEs to classify all of the subsystems of an IC TOE at the level of the high-level design as SFR-enforcing.

For example Test-ROM firmware could be classified as “SFR-non-interfering subsystem” because it does not contribute to the SFR (but is necessary for the manufacturer test) and is deactivated in the operational phase of the TOE. Another example, depending on the specific security functionality of a TOE, may be a standard peripheral unit, e.g. a timer, if separation can be shown.

Evidence of how the SFRs are provided

The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements (cf. ADV_TDS.x.2E). Assigning the SFR to subsystems or even modules may be especially difficult, since individual components not only provide the realization of a single SFR and very strong interactions and dependencies between components may exist. Mapping of the SFR of the ST via the Functional Specification to physical subsystems and modules may not be easy to do as mentioned above. For this reason, a description of the functional flow of security functions implementing the SFR to defined subsystems is of particular significance.

The SFRs of the ST expressing security properties might be realized and traced to technological properties of the TOE as described in the design.

Semi-formal notation
At EAL5, the TOE design is required to be semiformal. The semi-formal description of the TOE design can take the form of block circuit diagrams or hardware description language documents (HDL – hardware description language). In many cases, however, a hardware description language would first be used at the Detailed Design level.

Meaningful graphical representations of the technical or technological properties as part of the security mechanisms of the TOE may be considered equivalent to semi-formal representation.

The informal documentation of the technical and technological properties, as well as their integration into the structure and the realization of security mechanisms are necessary.

2.5.4 Implementation Representation (ADV_IMP)

2.5.4.1 Objectives

The objective of these requirements is to determine whether the implementation representation is sufficient to satisfy the SFR of the ST and is a correct realisation of the TOE design in a form that can be analysed by the evaluator.

It is the least abstract representation of the TSF and captures the detailed internal workings of the TSF in terms of source code, hardware diagrams and/or hardware design language or layout data, etc., as applicable.

2.5.4.2 Input

The implementation representation shall be made available by the developer at all levels from EAL4**.**

2.5.4.3 Requirements

Implementation representation for security IC
The TOE implementation representation corresponds to the following:

- hardware diagrams for analogic blocks;
- HDL statements for all synthesised components;
- if applicable, source code for all dedicated/embedded software;
- physical design information like layout and mask plans describing the implementation of the physical components.

The complete implementation information and layout shall be made available to the evaluator in a form used by the development personnel. This will imply in specific cases that the evaluator uses the tools of the developer for examination of the implementation representation (e.g. simulation tools, layout viewer).

Layout plans (physical design) describe the organization of the physical components and the signal routing with regard to the process masks and determine the metallisation masks.

Mask plans are necessary for the technological process. The mask plans need only be shown in certain cases if they are necessary for follow-up analyses like vulnerability analyses.

Layouts are required to check the correctness of the implementation of technical and technological properties. The layout indicates the ease with which physical attacks can be mounted (for example, the accessibility of the metallisation layer).

The technical and technological structure of the TOE is to be refined, in order to make an effectiveness analysis possible during the examination of physical attacks on the TOE (e.g. layout information about specific cells might be necessary if they are subject to certain attacks like FIB).

Adjustment of production process parameters will be determined at this stage via consideration of technology specific characteristics and the means of CAD tools.

Sampling of correspondence between TOE design and implementation representation of the TSF
An analysis of the implementation representation is performed by the evaluator with two objectives:

- analyse the correctness of the implementation representation and the TOE design, i.e. traceability of mechanisms implementing the SFR, and the security architectural principles of TSF self-protection, domain isolation, non-bypassability and secure initialization). This analysis uses the mapping between the TOE design and sampled or entire implementation representation in form of schematics/layout shall be provided for this purpose;

- understand the TOE implementation in order to specify potential vulnerabilities and attack paths.

At EAL4 (ADV_IMP.1) the evaluator would selects those parts of the TOE design description that are interesting (especially those crucial for the vulnerability analysis) to verify the implementation representation accurately reflects the description provided in the TOE design description.

In respect of implementation understanding at level ADV_IMP.1 in respect of implementation understanding, the compiling chain from TDS TOE design to the IC the sample of the TOE implementation, shall be documented, provided and their correspondence demonstrated (ADV_IMP.1.2D and ADV_IMP.1.3C). To support the correspondence analysis between TOE design and implementation representation, layout information as well as TOE design deliverables for subsystems and modules should be used. Links between TDS documentation and analogic blocks shall be described and interfaces documented

For example, an FPT_TST.1 (self-tests at start-up and periodically thereafter) requirement may be achieved by environmental sensors, which in turn are represented by security logic and hardware schematics. In this case, operational envelope conditions would need to be traced through the various levels of FPT_TST.1 representation and test evidence.

At level ADV_IMP.2 the required description of relationships between the entire implementation representation and the TOE design shall include justification of relations between modules and the technical and technological structures of the TOE as well as between hardware and firmware parts of the TOE.

2.5.5 TSF internals (ADV_INT)

2.5.5.1 Objectives

This family ADV_INT addresses the assessment of the internal structure of the TSF. A TSF whose internals are well-structured is easier to implement and less likely to contain flaws that could lead to vulnerabilities; it is also easier to maintain without the introduction of flaws.

2.5.5.2 Input

The developer shall provide an internal description and justification. The developer shall design and implement the entire TSF such that it has well-structured internals at EAL5 to EAL7.

2.5.5.3 Requirements

The property “well-structured” depends on the specific technology used for the TOE and typically originates from industry standards for this technology discipline. The CC part 3, section A.3, and the CEM, section 11.6.1, describe criteria to judge about this property for software. For hardware parts of the TSF represented in hardware description language (HDL) the similar criteria apply as for software.

The TSF of security IC is well-structured if the TSF structure provides for minimisation of the complexity of:

- the logical and physical interfaces between modules in a way that the TSF design provides for largely independent modules that avoid unnecessary interactions;
- the functionality in the module, which allows the evaluator as well as the developer to focus only on that functionality which is necessary for SFR enforcement, contributing further to understandability and further lowering the likelihood of design or implementation errors..

The CC Part 3, section A.3.1, characterizes modularity of software as follows: *“software written with a modular design aids in achieving understandability by clarifying what dependencies a module has on other modules (coupling) and by including in a module only tasks that are strongly related to each other (cohesion)”*.

A maximal independence of modules (described according to ADV_TDS.3 or higher) within an IC TOE could be possible if there were no or only minimal physical overlaps and logical dependencies between the individual modules and the interfaces are clearly defined. There are interfaces, which are necessarily complex and cannot be minimized for example buses.

Note the requirements for well-structured internal structure of the TSF do not contradict security IC layout, which hides the structure on the implementation level to increase the barrier for physical attacks (e.g. random module placement, glue logic).

The developer justifies the characteristics used to judge the meaning of “well-structured” used in the internals description and the development process. The evaluator shall examine the justification to determine that it identifies the basis for determining whether the TSF is well-structured (cf. work unit ADV_INT.1-1). The acceptance of the TOE specific criteria for being well-structured should be agreed with the evaluation authority before performing an analysis.

2.6 Security policy modelling (ADV_SPM)

2.6.1 Objectives

The evaluation of Security Policy Models (SPM), applicable for EAL6 and EAL7, is mainly concerned with formal security policies.

Hence the objective of the requirements is twofold: to determine whether the security policy model clearly and consistently describes the rules and characteristics of the TOE Security Policy and to reinforce the description by formal proof.

The security policy model is considered to structurally formalize the security functionality with sufficient explanatory text as well as to provide the necessary framework to carry out the formal proof of correspondence between the functional specification and the respective policies of the security policy model.

To this end the Security Policy Model of the TOE is informally abstracted from its realization by considering the proposed security requirements of the ST. The informal abstraction is taken to be successful if the TOE's principles (aka rules) turn out to be enforced by its characteristics (see ADV_SPM.1.2C). The purpose of formal methods lies within the enhancement of the rigor of the enforcement; informal arguments are always prone to fallacies, especially if relationships among subjects, objects and operations become more and more involved. In order to minimize the risk of insecure state arrivals the characteristics and rules of the SPM are therefore mapped to their formal counterparts as features and properties within some formal framework, whose rigor and strength can afterwards be used to derive the security properties in terms of theorems.

As structured representations of security policies of the security policy models are therefore used to provide increased assurance that the functional specification corresponds to the security policies of the security policy model, and ultimately to the TOE security functional requirements.

The formal counterpart in terms of principles and features therefore supports the correspondence mappings between the functional specification, the security policy model, and the security policies that are modelled.

2.6.2 Input

The developer shall provide a TOE Security Policy Model at EAL6 and EAL7.

2.6.3 Requirements

The formal security model is a formal description of the security policy using appropriate formal languages. It is utilized at an abstract level independently from the TOE implementation in hardware or software.

As a guidance on the formality requirements for technical and technological properties (e.g. difficulty of reverse engineering, or operation out of envelope) it may help to model the protection of the IC against unauthorized disclosure of assets, unauthorized use of assets, and unauthorized modification of assets in terms of barriers in combination with the security states of the IC during the different life cycle phases. In many cases a finite state machine seems best suited to satisfy the requirements.

Typically the developer determines the assets beforehand and uses an abstraction appropriate to take care of all desired security functionality. He/she may choose to subdivide the IC operations into security states (e.g. user mode vs. system mode) and state transitions together with subjects acting on objects and causing the state transitions to occur. As the cause of events is proceeding with time the formal system should be at least as strong as to implement mathematical induction to exclude the possibility of insecure state arrivals.

Formal systems appropriate for ADV_SPM.1 include (but are not restricted to) B-Method Isabelle, MetaMath, and VSE II. The formal system shall be agreed with the Evaluation authority of the concrete evaluation process.

The CC does not require that all security functionality be formally modelled, only those policies that can be modelled according to the state of the art. However, Information Flow Control and Access Control almost always are included within the formal model and strong arguments are needed in order to abstain from considering these policies.

2.7 Tests (CLASS ATE)

The assurance class ATE states testing requirements that demonstrate that the TSF satisfies the TOE security functional requirements. The CC distinguishes four assurance families within this class: Test coverage (from EAL2), test depth (from EAL3), functional tests (from EAL2) and independent tests (from EAL1). Note that testing addresses also mechanism defined in ADV_ARC in depth of testing.

2.7.1 Coverage (ATE_COV)

2.7.1.1 Objectives

The objective of these requirements is to determine whether the testing (as documented) is sufficient to establish that the TSF has been systematically tested against the functional specification. Coverage deals with the completeness of the functional tests performed by the developer on the TOE.

2.7.1.2 Input

The developer shall provide evidence (at ATE_COV.1, EAL2) / an analysis (from ATE_COV.2, EAL3) of test coverage. This analysis may be part of the test documentation itself or supplied separately.

2.7.1.3 Requirements

The test coverage analysis shall consider the mapping between tests (characterization and production tests) and the TSF as described in the functional specification (security functions). The coverage analysis shall show that all properties of the security functions are covered.

The analysis has to show and justify whether the TOE has been comprehensively tested. Complete coverage of security functions and external interfaces is required at EAL3 and higher (ATE_COV.2). From ATE_COV.3 (EAL6) the analysis has to show that all external interfaces have to be completely tested. For an IC, this can mean for example that the complete instruction set of the CPU with all parameters be covered.

Regarding test coverage, attention must be paid to the inclusion of security functions which result from design or technology. Therefore, evidence has to be provided that technical and technological properties specified in the FSP are covered by tests or other appropriate activities (e.g. layout, mask and chip inspections).

2.7.2 Depth (ATE_DPT)

2.7.2.1 Objectives

The objective of these requirements is to determine the depth of testing. Depth analysis deals with the level of detail to which the developer tests the TOE. Testing of security functions is based upon increasing depth of information derived from analysis of the TSF representations, e.g. whether the developer has tested the TSF against its high-level design at EAL3.

2.7.2.2 Input

The developer shall provide an analysis (from ATE_DPT.1, EAL3) of test depth. This analysis may be part of the test documentation itself or supplied separately.

2.7.2.3 Requirements

The depth of testing analysis which is provided for these requirements shall consider the mapping between tests (characterization and production tests) and internal structures of the TSF. Depending on the level of evaluation, this is done at:

- the basic design level (ATE_DPT.1, at EAL3);
- the subsystems and security enforcing modules design level (ATE_DPT.2, at EAL4);
- the subsystems and modules level design level (ATE_DPT.3, at EAL5 – EAL6);
- the subsystems and modules design level and the implementation representation level (ATE_DPT.4, at EAL7).

The application of depth of testing analysis will depend critically on how the terms “subsystems” and ”module” are used for an IC (cf. CC Part 3, para. 276 and 277, and section 2.5.3.3, Basic structure of the TSF in terms of subsystems and modules).

All deliverables provided at a certain level (e.g. block diagrams, HDL code, layout documents) should be used for examination of test depth.

For ATE_DPT.3, appropriate depth of testing is achieved when all instructions and branches of the whole logical plan vs. HDL source code, which belong to the SFR enforcing modules, have been tested.

The correctness of the implementation (integration) and the test coverage must also be proven after production (see ATE_FUN). The test vectors must be chosen appropriately, so that they cover the requirements. Analyses should be performed in this way.

The justification for test depth on the implementation level can be done with respect to one of the following items:

- The developer can, if possible, show that he has toggled each junction of a module during testing.
- If, according to the logical plan, the modules or parts of them can only be tested in parallel, the developer must show that all junctions have been toggled at least once via the underlying test vectors.
- If the developer has not taken testability rules into consideration, or the testing of some modules is not immediately possible (the testing of a timer over 24 hours), the circuit cannot be considered 100% tested. In this case, test coverage is achieved if the developer can show that all junctions were achieved via the test vectors and that there are no conditions which compromise security.

If using EAL4 for an IC evaluation, augmentation of EAL4 by the component ATE_DPT.3 might be sensible to get higher assurance, because the low-level design has been provided anyway and in case of testing technical and technological properties, a low-level design view of tests is sensible.

2.7.3 Functional tests (ATE_FUN)

2.7.3.1 Objectives

The objective of these requirements is to determine whether the developer’s functional testing demonstrates that all TSFI perform as specified.

2.7.3.2 Input

The developer shall test the TSF and document the results. The developer shall provide test documentation. For the conduct of tests, IC data sheets are of particular importance.

2.7.3.3 Requirements

The developer test documentation is required to give details of test plans, goals, and results (actual and expected). Because ATE_FUN.1 is used at EAL2 to EAL5, the quantity of information that must be presented will vary in accordance with the use of ATE_COV and ATE_DPT.

Tests of individual components of the TOE, or the control of certain technical or technological properties, could only possibly be implemented at a certain time during the manufacturing process or only in test mode, since the respective physical components can be neither logically nor physically accessed after the end of the production of the TOE. This should be considered during test planning and be appropriately documented.

Test plan

The test plan has to show the objective of the tests, which are to give evidence for the correctness of the logic by means of simulation using the HDL tool and to test the correctness of the implementation. Since a test is a type of quality control, after simulation it must be proven whether the implementation has been successful. Individual tests on the finished IC must show that the implementation of the TSFI and mechanisms is correct, and that the timing requirements are fulfilled. During testing specified functionality or during module testing, binding of modules is of particular note, especially if parallel functionality exists.

Typically, the two main steps in testing a hardware TOE are:

- the ”TOE prototype” tests;
- the acceptance tests performed on each TOE at the end of the production phase.

"TOE prototype" tests are characterisation tests that can be considered to provide evidence for the correct implementation of security enforcing functions. Timing should be considered when testing Hardware TOEs. Tests can also be implemented at the design level with the help of HDL tools (without delays, with estimated loads/ delays and post-layout as appropriate) or in form of special security tests after production using e.g. specific software residing in the TOE (test software within the ROM and being part of the TOE or application test software in the EEPROM not part of the TOE).

Acceptance tests have to confirm and verify the correct operation of the TOE and the components of which it is constructed during its manufacture. Therefore, the evaluators shall check the developer’s manufacturing process that it has appropriate acceptance tests implemented. The acceptance testing during production is usually performed using specific hardware mechanisms and commands implemented in the test software on the chip.

The different test environments used for evaluation shall be described within the test plan, e.g.

- ”TOE prototype” tests:
  - characterisation test environment
  - design simulation environment during development
  - security testing environment
- acceptance testing environment during production.

Equipment, which is necessary for a test case, must be specified exactly with all adjustments. This also includes the precise identification of the test libraries for simulation as well as the driver program for the test equipment.

In order to perform or to check the results of characterisation and acceptance tests where specialist test equipment is essential, the evaluator may have to witness and verify the tests rather than personally perform them. This is normally done through a visit to the IC designer/manufacturer.

If the developer would like to do security testing without simulation by means of the HDL tools, all tests must be carried out in real time in order to give evidence that the implementation be correct.

The library of test programs provided by the developer shall contain test programs and tools to enable all tests covered by the test documentation to be repeatable (required for ATE_IND). This may include driver software, among other things, with its associated equipment (tester) required for the testing of the chip. This is also necessary for repeating tests. Other tools that have been used, such as the logic analyser, oscilloscope, debugger, operating system etc. also need to be stated.

A test plan determines the framework of the test cases. In the test plan, the exact specification and scope of the test cases, as well as the documentation describing all input and environment parameters of the IC, are of great importance. These parameters are partially given in data sheets. Therefore the data sheet must be an integral part of the test documentation.

The test cases can vary greatly with analogue and digital circuits.

The test plan should cover all configurations of the IC if specified for the operational environment, e.g. different security states of the IC like test mode and user modes depending on the life cycle phases under evaluation.

Apart from the functional tests under standard conditions, tests (if necessary real time tests) under defined stress conditions (temperature, frequency, voltage, EPROM cycle tests etc.) are also to be planned, since such conditions could arise during the operation of the TOE (comparable with extreme situations for software TOEs, which could lead to run-time errors).

If during operation of the TOE external HW or SW functionality be included dynamically in the functional flow, then the relationship of the external components to the level of the external interface should be tested.

A mapping shall be given between the test cases and TSFI and subsystems, modules or interfaces under test depending on test coverage and depth.

Test parameters must be taken into consideration in the test planning. They could be for example:

- test frequencies with minimum and maximum limits
- voltage supply corresponding to the data sheet
- test temperatures
- test vectors for the selection of the test areas in the IC

Test results
The way test results are presented by the hardware must be described (e.g. written to a register or certain memory area, sent via an external interface line).

The test results, which will be obtained on special test equipment, must be presented in a form that can be analysed (analogue tests, timing tests).

For test results concerning functionality which run in parallel, the assignment of the results to specific subsystems, modules or security mechanisms is of significance. The dependencies of the results of the tests resulting from parallel processing functionality should be explained.

2.7.4 Independent testing (ATE_IND)

2.7.4.1 Objectives

The objective of these requirements is to determine whether the TOE behaves as specified and to gain confidence in the developer's test results by independently testing a subset of the TSF and by performing a sample of the developer's tests by a party other than the developer (e.g. a third party).

This family adds value by the introduction of tests that are not part of the developer's tests.

2.7.4.2 Input

The developer shall provide the TOE (from ATE_IND.1) and an equivalent set of resources (from ATE_IND.2). The evaluator shall provide test documentation.

2.7.4.3 Requirements

The equivalent set of resources the developer has to provide from ATE_IND.2 may include a separate sample of chips from production, a separate set of test vectors and a separate set of test data necessary for testing.

The evaluator shall provide test documentation. Requirements for test documentation are comparable to those for the developer's test documentation in terms of a test plan, procedures, and expected and actual results.

From the expertise point of view, the evaluator must be able to repeat the developer's tests and perform additional tests. For the conduct of tests, the evaluator needs test vectors, which determine the course of tests. If required, the evaluator must be in the position to use the tools for evaluation applied by the manufacturer. In many cases, owing to tool availability, this will only be possible in the development laboratory or during production by the manufacturer. In these cases, it is sufficient for the evaluator to witness the tests at the manufacturer's site.

Apart from the functional tests under standard conditions, tests (if necessary real time tests) under defined stress conditions (temperature, frequency, voltage, EPROM cycle tests etc.) are also to be performed by the evaluator, since such conditions could arise during the operation of the TOE and may not be extensively tested by the developer.

The additional evaluator tests must be performed at least at the level required by ATE_DPT.

The evaluators must also perform additional tests on a completed IC (final part), because:

- errors could be introduced by technology and may not be detected by logic tests (cf. the ageing process in paragraph 322);
- the scattering of security-enforcing and security-relevant parameters cannot be tested via simulation. Such scattering can only be carried out by means of testing several ICs. In order to do this, the evaluator has to select an appropriate sample or rely on the results of the manufacturer's quality tests. For example, the scattering of a mistake in digitalisation can only be detected if several ICs are tested, as assembly of basic components can lead to a timing deviation.

2.8 LIFE CYCLE SUPPORT (CLASS ALC)

Assurance class ALC defines requirements to determine the adequacy of security procedure that the developer uses to protect the TOE development and manufacturing environments. These procedures include the life-cycle model, the configuration management, the handling of security flaws, the tools and the security measures used throughout the TOE development, and the delivery activities.

As defined in CC Part 1 §139, 'Development' means here development and production.

2.8.1 CM capabilities (ALC_CMC)

2.8.1.1 Objectives

Configuration Management Capabilities defines the requirements to ensure that the developer has clearly and uniquely identified the TOE using an automated configuration system. The CM system ensures that the TOE is correct and complete during evaluation and before sending to the customer, and prevents any unauthorized modification, addition or deletion of the configuration items.

2.8.1.2 Input

EAL4 and EAL5 levels require ALC.CMC.4.

The developer shall provide CM documentation that includes a CM plan.

2.8.1.3 Requirements

The CM plan shall describe how the CM system is used (ALC_CMC.4.7C), and how the TOE configuration items modification or addition are controlled (ALC_CMC.4.8C) with automated measures (ALC_CMC.4.4C).

The CM system shall be able to automatically generate the TOE (ALC_CMC.4.5C)

The TOE shall be labelled with a unique reference (ALC_CMC.4.1C) and all configuration items shall be uniquely identified. (ALC_CMC.4.3C)

The configuration system and the acceptance procedures should be considered during the whole development and production process of the TOE. They must be in a position also to control the construction plans and hardware parts, in addition to all relevant data files for all development steps. If applicable, various development and production sites are also to be included in this.

The evaluator should ensure that the TOE contains a unique reference such that it is possible to distinguish between different versions of the TOE. The TOE may provide a method by which it can be easily identified. For hardware TOEs this may be a part number physically stamped on the TOE. Furthermore, each TOE mask layer may be physically identifiable by use of any kind of identifiers.

However, in certain cases it can be necessary, in order to make an attack more difficult, to mark the ICs (or the chips held within the ICs) with non-visible logos or IDs. In such cases, the manufacturer must, however, find a suitably hidden possibility for the label on the TOE, such as for example, in a non-deletable area of memory with access for authorized users only.

The evaluators work unit at ACM_CMC.4.5C/EAL4 to examine the TOE generation procedures has the objective to get evidence about the effectiveness of the configuration control system with regard to the various versions and changes to the TOE. It has to be shown that the configuration control system supports the generation process to help reduce the probability of human error. Thus, the generation process makes use of the appropriate design tools (HDL / CAD tools). This should be described.

In the case of an IC TOE comprised of hardware and software (e.g. Test-ROM software, operating system, smart card application software depending on the specific scope of a TOE) there is likely to be a distinction between the hardware and software configuration control. There is an additional requirement to bring together the right hardware-software pair, which means that the right mask must be used. This in turn means that the configuration control system must be able to administrate hardware-software pairs comprising a TOE. Because all masks are created from mask data files it has to be ensured that masks are created from their correct software image.

Depending on the scope of the TOE, bringing together the right hardware-software pair can partly be an aspect of the TOE configuration management or of the delivery procedures (see ALC-DEL).

It is not possible to relate this work unit for generation of the TOE directly to the technological process of a customer specific IC, because the process cannot be repeated for the benefit of the evaluator. In this case, the evaluator must, however, audit the configuration control in the technological process in order to guarantee that the correct masks, which belong to a particular version of the TOE, are used and organizational measures are effective in the process.

In the case of programmable standard ICs (PLD, FPGA), in which the hardware configuration is programmed via firmware, the work unit may be supported by programming a new IC. The evaluator then conducts comparison tests of the functions of the newly produced IC with the original TOE (to be equated with a ‘file compare’ for a re-built software TOE).

2.8.2 CM scope (ALC_CMS)

2.8.2.1 Objectives

The objective of these requirements is to identify the items to be included in the configuration list and hence placed under the CM requirements as per ALC_CMC.

2.8.2.2 Input

EAL4 requires ALC_CMS.4 , EAL5 requires ALC_CMS.5.

The developer shall provide the TOE configuration list.

2.8.2.3 Requirements

The configuration list shall include the TOE itself, the evaluation evidences required by the SARs, the parts that comprise the TOE, the implementation representation, the security flaw reports and resolution status (ALC-

CMS.4.1C). Additionally for EAL5 level, development tools and related information shall be considered in the configuration list (ALC_CMS.5.1C).

The developer performs configuration management on the TOE implementation representation (hardware schematics/layouts), design documentation, tests, user and administrator guidance, the configuration management documentation and security flaws with flaws resolution status.

Configuration management shall be in place for IC design (schematics, layout) as well as IC proprietary dedicated software (source code, documentation). All source files necessary for the generation of the TOE as well as the identification of the set of masks necessary for the manufacturing of the TOE have to be included. For masks, this includes unique mask identifier, as well as the version number or revision number of each layer.

Because the configuration control system must be able to administrate hardware-software pairs as part of the TOE (see ALC_CMC), there must be evidence at ALC_CMS which specific hardware-software pair is used for the TOE.

The identification and listing of modules of the design in the configuration list seems to be difficult to apply to ICs. Since, within the framework of the design, functional blocks can be taken out of a developer’s HDL or CAD library and out of the IC manufacturer’s technology library (lists of the technology parameters). At the very least the libraries as a whole that are used, together with the possible parameters that are used, must be clearly identified if individual library components do not have their own identifier.

Test information covered by CM shall include all of the parts which are necessary for the generation and testing of the TOE. That includes all test equipment, libraries, and the list of test vectors used during testing as well as the set of tests including test data and results.

ALC_CMS.4.3C and ALC_CMS.5.3C requires the configuration list to indicate the developer of the item. As defined in CC3.1 Part 1 §138, "Developer" here refers to the organisation responsible for the development of the item. That is e.g. any developer of an additional software-part (library) to be used by the TOE (see CC 3 Part 3 §352). The intention is to give evidence on the origin of parts of the TOE provided from external suppliers or if the development is done within different organizations.

2.8.3 Delivery (ALC_DEL)

The assurance family ALC_DEL defines requirements for the measures, procedures, and standards concerned with secure delivery, of the TOE, ensuring that the security protection offered by the TOE is not compromised during transfer.

2.8.3.1 Objectives

The objective of these requirements is to determine whether the delivery procedures are documented and maintain integrity and the detection of modification or substitution of the TOE when distributing the TOE to the user’s site. It includes special procedures or operations required to demonstrate the authenticity of the delivered TOE. Such procedures and measures are the basis for ensuring that the security protection offered by the TOE is not compromised during transfer.

2.8.3.2 Input

The developer shall provide delivery procedures of the TOE or parts of it to the user. The procedures shall be described and used.

2.8.3.3 Requirements

Requirements address delivery to Users. As per CC Part 3 § 365, transportation from subcontractors to developers or between different sites is not considered, but in ALC_DVS.

The examination of the delivery process to determine that the delivery procedures are used is normally done during site inspections. Traceability of what has been delivered by who to whom is verified. A particular attention is placed on ”parallel deliveries” such as samples for quality inspection, scrapped samples, screened processes.

If applicable, delivery procedures approved by the national certification body should be followed.

Note that a specific authentication mechanism (e.g. fab-key, transport key) may be used to protect the delivery of the chip from the chip manufacturer to the Card Manufacturer/personalization centre.

For ICs the security state of the chip (test mode, user mode) during delivery is of importance. Functionality for the deactivation of test hardware or for the transition from test mode or installation mode to user mode/operational mode is important in the context of vulnerability analysis and the authenticity of the delivered TOE. It should be mentioned here with reference to the description in AGD_PRE.

The TOE manufacturing and delivery process shall include production tests that ensure the correct function of each TOE example delivered to the costumer. The results of these tests must be documented.

2.8.4 Development security (ALC_DVS)

2.8.4.1 Objectives

The objective of these requirements is to determine whether the development and manufacturing environment procedures are adequate to provide the confidentiality and integrity of the TOE design, implementation and production that is necessary to ensure that secure operation of the TOE is not compromised.

2.8.4.2 Input

The developer shall provide development security documentation.

2.8.4.3 Requirements

ALC_DVS.1.1C requires that documentation describes all security procedures used to protect the TOE during development. ALC_DVS.2.2C additionally requires that the documentation justifies that security measures provide the necessary level of protection.

Note that ALC_DVS gives the possibility to define the level of security in Confidentiality and Integrity. Referring to CC Part 3 §14.4 374 " *It is recognised that confidentiality may not always be an issue for the protection of the TOE in its development environment. The use of the word "necessary" allows for the selection of appropriate safeguards*. " For instance for 'open source software', no confidentiality is required.

During the life-cycle of the hardware TOE, development and manufacturing security procedures are examined. All relevant development and production sites of the TOE must be taken into consideration so that the security requirements are valid for all life cycle phases until the final delivery of the TOE within the scope of the evaluation. This is of particular importance because the requirements on the technology are finally only realized during the production of the ICs, including tests for correct function of all TOE examples delivered to the costumer. The examination includes all the steps of the development and manufacturing process; the following sites are concerned:

- development of dedicated software and hardware (design centre),
- site for creating the image of the application software (if applicable),
- reticles manufacturer (mask manufacturer),
- manufacturing (fab site),
- testing (test site),
- packaging (microassembly and testing) depending on the scope of the TOE.

In specific cases there may be a separate design centre for certain cells that are not TOE specific (e.g. standard CPU cell, standard memory cell). For the requirement ALC_DVS.1, there may be enough evidence that these pre-defined cells (not security enforcing but possibly security supporting) are functionally correct and integer if appropriate delivery procedures, tests and confidentiality agreements are in place. In this case this design centre would not have to be considered under ALC_DVS. The site of the mask manufacturer can be treated accordingly.

All the security operational procedures are being checked. The examination is normally done during site inspections. Subcontractor procedures are also checked. It should be noted that evaluator access to manufacturing site, specialist personnel and tools would be required to support these evaluation activities.

The Procedures shall include the following types:

- physical (site security: access controls);
- procedural (granting of access to the development tools, revocation of access, transfer of protected material, admitting and escorting visitors, development security policy ...);
- personnel (screening process for new development staff ...);
- IT security measures (Identification and authentication, access control, archiving, audit, networking, firewalls ...).

Further sensitive areas within the sites mentioned above might be:

- process control (integration of the circuits onto silicon);
- product engineering (fault analysis with regard to the process);
- quality control for security functionality;
- storage / delivery.

The TOE is present in the various stages of development and production in various different physical shapes. The integrity of the layout masks is of particular significance. Secure delivery will support this aspect (see ALC_DEL).

Physical, procedural, personnel and other measures necessary for the realization of the TOE's security properties, as given in the Security Target, will be transposed in the development and production and will have an effect on the security in the operational phase of the TOE. These measures are also to be documented and examined. Measures in the test phase, as well as the assembly phases if applicable, and measures for the management of the manufacturing process are particularly important.

In comparison, compilation of a software TOE takes place with fixed options uniquely in the development environment (prototype and master copy). The series production of the software is simply a process of copying, in which the integrity aspects of the copy with respect to the master copy play a role.

With respect to IC TOEs, drawings and associated data files will be created within the framework of the development. The IC production of the prototype as well as the series is essentially more complex than a copying process in the case of software and is variable through a multitude of process parameters, which are potentially manipulated by personnel.

The test phase during IC production is of particular importance, since in this phase an IC is already completely physically available, but, for example, internal IC structures are, however, adjustable or may be compromised via a test mode, which is still activated.

Measures, which are taken, in order to mark (ink) the faulty dice on the wafer and to sort out faulty TOEs (final parts), including which criteria to select, can be of importance. Measures for the destruction of defective parts should then be described.

2.8.5 Flaw remediation (ALC_FLR)

2.8.5.1 Objectives

Flaw remediation ensures that flaws discovered by TOE consumers will be tracked and corrected while the TOE is supported by the developer. While future compliance with the flaw remediation requirements cannot be determined when a TOE is evaluated, it is possible to evaluate the procedures and policies that a developer has in place to track and repair flaws, and to distribute the repairs to consumers.

2.8.5.2 Input

The developer shall document the flaw remediation procedures.

2.8.5.3 Requirements

This CC family is not mandatory for the predefined EAL packages. Nevertheless, it is possible to select one of the ALC_FLR assurance components within the ST by EAL augmentation.

Aspects of flaw remediation might be combined with the use of an evaluation maintenance programme.

2.9 Life Cycle Definition (ALC_LCD)

2.9.1 General Remarks

2.9.1.1 Objectives

The objective of these requirements is to determine whether the developer has used a documented model of the TOE life-cycle for development and maintenance.

Life cycle definition establishes that the engineering practices used by a developer to produce the TOE include the considerations and activities identified in the development process and operational support requirements.

Confidence in the correspondence between the requirements and the TOE is greater when security analysis and the production of evidence are done on a regular basis as an integral part of the development process and operational support activities. It is not the intent of this component to dictate any specific development process.

2.9.1.2 Input

The developer shall provide a life-cycle definition (from EAL4).

2.9.1.3 Requirements

The description of the model should include information on the procedures, tools and techniques used by the developer for development and maintenance of the TOE.

An example of the life-cycle model is detailed in the Security IC protection Profile [BSI-CC-PP-0084-2014]. This model shall be refined by the developer.

A basic description is required at ALC_LCD.1 / EAL4 to EAL6, whilst at ALC_LCD.2 / EAL7 the life-cycle model used shall be based on a measurable life-cycle model, i.e. one that has been approved by academic experts or standards' bodies.

2.9.2 Tools and techniques (ALC_TAT)

2.9.2.1 Objectives

The objective of these requirements is to determine whether the developer has used well-defined tools to develop, analyse and implement the TOE (e.g. programming languages or computer-aided design (CAD) systems) that yield consistent and predictable results.

It includes requirements concerning the development tools and implementation dependent options of those tools.

2.9.2.2 Input

The developer shall provide development tools' documentation being used for the TOE (from EAL4).

2.9.2.3 Requirements

The evaluation aspect for tools and techniques is applicable to software as well as hardware TOEs.

When considering tools and techniques for software TOEs, it is a question of getting evidence whether the development tools which have been used are unambiguously and well defined and documented, and whether all options of the tools have been documented. From ALC_TAT.2/EAL5 implementation standards have to be applied. The objective here, apart from a higher assurance into the correct implementation of the TOE, is also to ensure repeatability of the construction of the TOE. The required confirmation of the evaluator that the implementation standards have been applied may require visiting all relevant sites. Therefore, it should be noted that evaluator access to manufacturing site, specialist personnel and tools would be required to support these evaluation activities.

For the dedicated software of the IC, this corresponds to the software development tools.

The use of the development tools shall be documented. This includes in particular the description of the compiling chain for the software source code (if applicable) and the synthesis chain for HDL. All options shall be documented and parameters shall be clearly identified. The evaluator shall verify this tools' chain, usually during site inspection.

In order to achieve the objective of ALC_TAT for a hardware TOE, it is necessary to document and test the hardware description languages (HDL), representation elements (graphical logic elements) and tools (e.g. HDL-compiler, simulation tools, and CAD tools) used in the hardware. Additionally supporting libraries shall be considered. A clear and precise definition of all elements and the options used for the TOE is important.

In the case of software, various compilers can create different object codes even with the same functionality of the TOE (i.e. with the same logical design). Functionality is defined by the processor commands and the compiler options that are used.

In the event that microchip ICs have different masks, differing physical implementations can arise as a result of different technologies, even though functionality may be the same (i.e. with the same logical design at the level of the circuit diagram). Functionality is defined finally only by means of the cell structure which has been implemented in the silicon. As a result of this, the technology used for the implementation of the chip has to be specified. At high assurance levels, the parameters of the technology used have to be documented.

For the purpose of clarification, the following table shows the development processes of hardware ICs and software:

Table 2 - Development processes of hardware ICs and software

Software	Hardware
Program text input via the editor for the creation of the source file. Syntax and semantics of the input language will be determined via the compiler.	Creation of the logical plan through graphic input via a CAD tool or text input via a HDL-Editor. Syntax and semantics of the graphics symbols are determined via the CAD tool and the technology. For the modelling and the simulation of the circuit design a HDL will be used.
In order to construct a functional software TOE, several steps are required: Determining the compiler and linker adjustments, in order, for example, to realise certain optimization possibilities. Compiling and linking of the source files to a program which is executable from a processor during its run time (object files as program data files, run time library, program code for a hardware memory). Testing and de-bugging within the framework of the compilation of individual source files as well as the whole TOE.	In order to construct a functioning IC from the design, several steps are needed: The construction of a netlist out of the logical plans and the synthesis of the gate structure as well as the test structure. The simulation of this logic at the gate level and at the level of the layout using timing defaults. The construction of the layout and the masks. The manufacture of the microchip from this masks after several process steps, which are dependent on the semiconductor technology used (e.g. 0.8_ìm CMOS-, BiCMOS- or Bipolar technology).

A programming language used is based on the features of a compiler, interpreter or assembler, while the logic which has been constructed using an HDL is finally only available after the conclusion of the technological process. Therefore, this assurance aspect is to be understood in the sense of ”Tools, Techniques and Technology”.

2.10 GUIDANCE DOCUMENTS (CLASS AGD)

The Common Criteria assurance components of the families AGD_OPE (Operational user guidance) and AGD_PRE (Preparative user guidance) “*describe all relevant aspects for the secure application of the TOE*.“

2.10.1 Operational User Guidance (AGD_OPE)

2.10.1.1 Objectives

The Operational User Guidance documents should provide only the information which is necessary for using the TOE. Depending on the recipient of that guidance documentation Operational and Preparative User Guidance can be given in the same document.

The TOE serves as a platform for the Security IC Embedded Software. Therefore the role of the developer of the Security IC Embedded Software is the main focus of the guidance.

2.10.1.2 Input

The developer shall provide guidance documentation. The datasheet of the IC could be considered to support these requirements.

2.10.1.3 Requirements

If the TOE provides security functionality which can or need to be administrated by the Security IC Embedded Software or if the IC Dedicated Support Software provides additional services, these aspects must be described in Guidance.

Most of the security functionality will already be effective before TOE Delivery. However, guidance to determine the behaviour of security functionality, to disable, to enable or to modify the behaviour of security functionality must be given if a configuration is possible after TOE Delivery (that means either by the Developer of the Security IC Embedded Software or by the Composite Product Manufacturer). This guidance is delivered by the TOE Manufacturer.

If the Composite Product (with the TOE as a major element) is used in a terminal where communication is performed through the interface provided by the TOE in combination with the Security IC Embedded Software then Guidance must be given to the developer of the terminal. This is information about the physical characteristics of the device, the interface and standard protocols if implemented by the TOE.

Guidance documents must not contain security relevant details which are not necessary for the usage or administration of the security functionality of the TOE.

2.10.2 Preparative User Guidance (AGD_PRE)

2.10.2.1 Objectives

Preparative user guidance is intended to be used by those persons responsible for secure acceptance and installation of the TOE as well as the secure preparation of the operational environment in a correct manner for maximum security.

2.10.2.2 Input

The Family AGD_PRE addresses the activities of the delivery acceptance procedures. For the hardware platform this comprises procedures that can be applied to identify the TOE and eventually to verify the authenticity of that part of the TOE.

2.10.2.3 Requirements

The TOE may be configured after production before the Composite Product is delivered to the consumer. In this case, these configuration aspects have to be considered.

The preparation may include e.g. the download of Security IC Embedded Software. If the TOE includes software that is delivered separately, the preparation includes integration of the IC Dedicated Support Software. The preparation also includes the configuration of the TOE according to the options described in the Security Target that can be changed after TOE delivery. The guidance documentation shall describe all relevant procedures.

2.11 VULNERABILITY ASSESSMENT (CLASS AVA)

The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE. It consists only of one family Vulnerability analysis AVA_VAN, which comprises all aspects of vulnerability assessment.

2.11.1 Vulnerability analysis (AVA_VAN)

2.11.1.1 Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

The levelling of the components of the AVA_VAN family is based on an increasing rigor of vulnerability analysis by the evaluator and increased levels of attack potential required by an attacker to identify and exploit the potential vulnerabilities.

2.11.1.2 Input

The vulnerability analysis is subject of the evaluator. The developer has to provide the TOE for penetration testing.

The evaluators use all information they got and consider all potential vulnerabilities encountered during the conduct of other evaluation activities. The vulnerability analysis is based upon analysis performed by the evaluator, and is supported by evaluator testing.

2.11.1.3 Requirements

General aspects of vulnerability analysis

The CEM, section B.1, identifies three main factors in performing a vulnerability analysis, namely:

a) the identification of potential vulnerabilities;
b) assessment to determine whether the identified potential vulnerabilities could allow an attacker with the relevant attack potential to violate the SFRs.
c) penetration testing to determine whether the identified potential vulnerabilities are exploitable in the operational environment of the TOE.

The assessment of TOE resistance against attack is subject of the analysis. Therefore, the evaluator can use the public available documentation on potential vulnerabilities and potentially flaws only as a basis for the analysis. The evaluator must consider also modifications and improvements of the known attacks to verify the resistance of the TOE. The detailed information on the TOE design can support the adaptation of attacks and support the analysis of the resistance against specific attack steps.

This work requires expertise and equipment as outlined in Annex 8, MINIMUM ITSEF REQUIREMENTS FOR SECURITY EVALUATIONS OF SMART CARDS AND SIMILAR DEVICES. At least the evaluator must perform penetration tests to such an extent that the overall rating of the attack path can be proven by the provided test results.

Development and operational vulnerabilities

Vulnerabilities can be introduced in both the construction of the mechanism itself, as well as through the production of technical and technological measures intended to counter threats. The effectiveness of the functionality depends on the technology used in the implementation phase. This must be taken into consideration in the vulnerability analysis.

Development of vulnerabilities takes advantage of some property of the TOE which was introduced during its development, e.g. defeating the TSF self-protection through tampering, direct attack or monitoring of the TSF, defeating the TSF domain separation through monitoring or direct attack the TSF, or defeating non-bypassability through circumventing (bypassing) the TSF.

Operational vulnerabilities take advantage of weaknesses in non-technical countermeasures to violate the TOE SFRs, e.g. misuse or incorrect configuration. Any ways in which the SFR may be deactivated, bypassed or corrupted should be analysed and assessed by the evaluator. This analysis must provide arguments as to why the vulnerability cannot be exploited within the TOE's environment.

The operational vulnerabilities are also to be considered in the context of the use of the chip by an operating system or an application developer. For instance, the security measures which should be taken in the application development and which influence the operation of the IC could possibly be exploited by an attacker (e.g. demands on external cabling, external technical parameters, or confidentiality measures).

The process of ageing the IC should be taken into consideration during vulnerability analysis. So, for example, the vulnerabilities of an IC TOE can lie in the semiconductor technology. E2PROM cells only withstand a restricted number of program cycles. The limitation of the number of possible delete and write cycles of a cell is an inherent vulnerability, which an attacker could possibly exploit. This kind of technologically based vulnerability analysis is new in contrast with software TOEs, and requires a vulnerability analysis relating to the technology and its implementation.

Typical vulnerabilities

For smartcards and similar devices, Annex 7, APPLICATION OF ATTACK POTENTIAL TO SMARTCARDS AND SIMILAR DEVICES is considered as basis for search of potential vulnerabilities. Other activities will be performed according to standard CC practice as documented in the CC, the CEM, and other EUCC documentation.

Hardware TOEs can be subject to vulnerabilities which can be exploited by physical tampering of the TOE. With respect to attacks which physically modify the internal technical structures of the TOE, it is a question of an indirect attack which needs to be examined in the context of a vulnerability analysis, since security features may be bypassed and therefore may lose their effectiveness. Such tampering could circumvent the effectiveness of other security mechanisms. Additionally, the binding of distinct components realized in mechanisms has to be taken into consideration. This aspect must be considered during vulnerability assessment and penetration testing.

Binding aspects should be considered during vulnerability analysis, owing to vulnerabilities, which may arise from problems in binding if the TOE's security functions are not mutually supportive or do not provide an integrated and effective whole. In particular, it addresses the issue of indirect attack against the IC, e.g.:

- physical connections between physical components in the form of signal paths and circuits;
- physical connections between physical components because of the layout (i.e. that information on the technical and technological implementation needs to have some influence in the analysis);
- dynamic interweaving in the timing behaviour of individual security functions or mechanisms;
- influence on binding through the setting of external signals on the microchip.

Some hardware security mechanisms are only effective in combination with additional software countermeasures in a composite product. Therefore additional vulnerability analysis of the security mechanism of the composite product is necessary as defined by Annex 6, COMPOSITE PRODUCT EVALUATION FOR SMART CARDS AND SIMILAR DEVICES. These hardware security mechanisms must be evaluated to such an extent that the composite evaluator is able to assess the combination of hardware and software. A related description must be included in the ETR for composition. Open samples may be used by the composite evaluator to tune the test bench for the composite product.

Penetration testing
The penetration testing consists of an analysis of the TOE based on potential vulnerabilities and potentially flaws that are available from the public domain and scheme specific documentation.

Attack potential quotation
One key aspect of the vulnerability analysis requirements is the notion of resistance to attack posed by attackers who have a particular attack potential (basic, enhanced-basic, moderate or high attack potential). The attack potential considered for a TOE evaluation is pre-defined by selection of a certain AVA_VAN assurance component in the ST.

The resistance to attacks to be provided by the TOE depend on:

- the assets to be protected and the perceived risk of compromise of those assets;
- the intended operational environment determining the perceived attacks and the factors like windows of opportunity;
- the perceived market requirements under consideration of costs for development, manufacturing and certification.

E.g. subscriber identity modules (SIM) stores the service-subscriber key used to get access to mobile phone networks. The value of this service for an attacker cloning the SIM under risk for being detected and blocked by the network operator may be low. In this case basic resistance of the SIM against cloning may be appropriate. In other cases like pay TV storing cryptographic keys used by many subscribers in undirected communication may require high resistance against attacks compromising such key.

Therefore, for security IC or smartcard evaluations, if the target EAL is less than EAL6 it may be appropriate to augment the assurance requirement with a higher AVA_VAN component.

Annex 7, APPLICATION OF ATTACK POTENTIAL TO SMARTCARDS AND SIMILAR DEVICES, gives mandatory guidance for the rating of the attack potential necessary to perform specific attacks. It is a interpretation for security IC based on CEM, annex B, considering the specific technology and operational environment as well as the need of information about the security during the operation usage phase like separate rating of identification and operation for risk management. Rating provides a measure of the weakest path required to determine IC secrets or tamper with the IC. In practice, this is likely to be the sum of various work functions (e.g. remove protective barrier, determine IC layout, decrypt data or extract EEPROM contents).

Different methods can be used to prove the rating:

- Performing penetration tests up to a specific step of the attack path that proves the possibility but require considerable additional effort for the exploitation. For example power glitches are performed to such an extent that the resulting faults are reproducible and the effect of the faults can be determined or reverse engineering is performed to such an extent that a specific part of the circuit can be verified without usage of design information.
- Comparing results of penetration tests with a test setup not available to an attacker with the results of penetration test with a test setup available to an attacker. For example a SPA/DPA analysis is performed with chosen values or specific configurations and compared with random values and the configuration under evaluation.
- Running automated tests for the same time period that is used in the rating. For such tests the functionality of the test setup must be verified beforehand. The results of such tests may be partly successful however they shall not include any results that show a direct vulnerability. For example each semiconductor is sensitive to light attacks. Therefore the complete surface of the device must be scanned to check for faults that may provide indications for further successful attacks.

According to the CEM, the attack potential calculation does not distinguish any more between the identification phase and the exploitation phase but within the community for smartcards and similar devices, the risk management performed by the user of CC certificates required clearly to have a distinction between the cost of “identification” (definition of the attack) and the cost of “exploitation” (e.g. once a script is published on the web). Therefore this distinction is kept in Annex 7 when calculating attack potential for evaluation of smartcards and similar devices. Although the distinction between identification and exploitation is essential for this type of products evaluation to understand and document the attack path, the final sum of attack potential is calculated by adding the points of the two phases, as both phases build the complete attack.

When using the rating tables from Annex 7 or CEM, annex B, justification shall be provided why the assertions or assumptions supporting the analysis are valid (e.g. why a certain level of expertise or certain equipment for an attack is applicable and no less).

30. ANNEX 4: SECURITY ARCHITECTURE REQUIREMENTS (ADV_ARC) FOR SMART CARDS AND SIMILAR DEVICES

PURPOSE

This annex provides requirements for the developer on how to apply the assurance requirements of the family ADV_ARC to the Technical Domain related to smart cards & similar devices. It defines what kind of information the developer documentation provided to fulfil the ADV_ARC family, hereinafter referred to as the "ARC documentation", shall contain and in which level of detail this information shall be provided.

It applies to both developers of security integrated circuits and developers of composite products, consisting of a hardware platform and embedded software (native software, closed operating systems with one or more applications, open software platforms and more).

It does not define mandatory tasks for the evaluator, but may serve as a guideline for his/her activities.

Further guidance may be provided as to illustrate with examples the type of information and level of detail to be provided in the ARC documentation.

PARTICULAR STATUS

None.

CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE

Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS.

1 BACKGROUND INFORMATION

CC Part 3 introduces the security assurance requirements (SAR) family security architecture ADV_ARC as follows:

"The objective of this family is for the developer to provide a description of the security architecture of the TSF. This will allow analysis of the information that, when coupled with the other evidence presented for the TSF, will confirm the TSF achieves the desired properties. The security architecture descriptions support the implicit claim that security analysis of the TOE can be achieved by examining the TSF; without a sound architecture, the entire TOE functionality would have to be examined."

A security architecture is a set of properties that the TSF exhibits; these properties include self-protection, domain separation, and non-bypassability. These properties are distinct from security functionality expressed by CC Part 2 SFRs because they largely have no directly observable interface at the TSF. Rather, they are properties of the TSF that are achieved through the design of the TOE and TSF, and enforced by the correct implementation of that design.

The security architecture also describes the TOE security functionality (TSF) initialisation, i.e. the processing that occurs in transitioning from the "down" state to the initial secure state, when power-on or a reset is applied.

The Technical Domain related to smart cards & similar devices presents specificities that have to be taken into account in the drawing up of the ARC documentation. The main characteristics are:

- a device belonging to this domain is a combination of a one-chip Integrated Circuit with embedded software implementing cryptographic services using secrets. The TOE could cover the full product or only a layer that includes the IC (an underlying platform);
- the TOE may start up in a low-function mode and then transition to the evaluated secure configuration. A transition from power off also happens each time the device is used by the final holder;
- in its operational environment an attacker might have physical access to the TOE through the physical port and the IC surfaces;
- a particular lifecycle.

2 GENERAL ASPECTS OF CONTENT AND PRESENTATION

The ARC documentation shall support the vulnerability analysis of the evaluator but it does not provide a developer vulnerability analysis.

The ARC documentation shall describe security domains and the secure initialisation process, and demonstrates self-protection and non-bypassability. The description shall focus on the use of security mechanisms put into place and their collaboration in order to achieve overall security. To this end the developer may analyse and conclude how the security features and countermeasures of the TOE are intended to resist the general attacks listed in Annex 7, Application of Attack Potential to Smart Cards viewed in the light of tampering and bypass.

Note: Using the ARC documentation, the evaluator will perform an independent vulnerability analysis to determine the actual resistance of the TOE to attacks. The evaluator will consider all potential vulnerabilities encountered while performing evaluator activities or found by independent methodical search. The evaluator will determine whether vulnerabilities are exploitable by an attacker possessing the attack potential addressed in the ST. Thus, the ARC documentation and the vulnerability analysis are different in responsibility, methods and result.

The security architecture description shall describe all properties of the TOE and the TSF and all security mechanisms of the TSF that contribute to enforce the security architecture. The security mechanisms specific for enforcement of security architecture properties may be fully described in the ARC documentation, or in the TDS documentation in which case the ARC documentation refers to these descriptions.

Note: some security mechanisms are spread across the whole implementation and cannot be expressed or are not easily expressible within TDS documents and mapping to modules. The description of the security architecture should avoid redundancy with other parts of ADV.

The CC require the security architecture description being at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document. But this does not imply the same rigor of the presentation in the ARC documentation; the use of semi-formal or formal methods is not required for the ARC documentation. Even though the CC require the developer to provide a mapping between the TOE design description and the sample of the implementation representation, such mapping is not required for the security architecture description.

Within the Technical Domain of smart cards and similar devices, the TOE physical boundaries are TSFIs. The device surface is the TSFI for physical protection against manipulation. The surface of the IC itself can output physical signals such as electromagnetic emanations that could be used for side channel analysis or input energy used for perturbation like laser attacks. The ports are physical entry or exit points of power supply and physical signals for the TOE that provides access to the TSF. The physical signal contains more information (e.g. timing, signal level) than the data intended to be exchange through the logically defined TSFI. The power supply port is not part of the logical interface but may affect the TSF (e.g. by glitches).

The evaluator is reminded that it is the synergy and not the distinction of self-protection, non-bypassability, domain separation and secure initialisation that are in the focus of the ARC documentation.

3 LEVEL OF DESCRIPTION IN ADV_ARC

ADV_ARC.1.1C requires the architecture description to be "*at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document*".

As the expected assurance level is EAL4 augmented by at least AVA_VAN.5, or higher, the level of description shall correspond to parameters, actions and error message for TSFI, the module interface level and in some case to implementation specific details. But semi-formal or formal description is not required because it does not bring more comprehensive details.

The security architecture description shall be based upon security mechanisms (SFR-enforcing entities, mechanisms enforcing the properties, design countermeasures, coding conventions). Each security mechanism shall be explained in terms of purpose and behaviour with the exception of SFR-enforcing entities that are described in decomposition documentation.

For Security Mechanisms spread across the whole implementation, it shall be ensured that there is little ambiguity between the description in ADV_ARC and ADV_IMP by providing the principles that have led to their implementation in the code. The security mechanisms description may be illustrated with code sample or example.

4 SECURITY DOMAINS

The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs (cf. ADV_ARC.1.2C).

Domain separation is a property whereby the TSF creates separate security domains on its own and for each untrusted active entity to operate on its resources, and then keeps those domains separated from one another so that no entity can run in the domain of any other.

The security architecture description shall explain the different kinds of domains that are created by the TSF, how they are defined in terms of resources allocated to each domain, and how the domains are kept separated so that active entities in one domain cannot tamper with resources in another domain.

If the TSF is the only active entity and there are only data structures maintained by the TSF to manage the interactions with the users, the security architecture will describe that there is no security domain available for active entities.

If the TSF provides security domains for other active entities, it shall protect these domains against adverse actions of these potentially-harmful entities on TSF resources. Moreover, the TSF will keep this domain separated from the security domain of other active entities.

If the ARC documentation describes security domains, the allocation and deallocation of the resources for the active entities should be under SFR control (e.g. FDP_ACC: access control). The use of the resources by the active entity in the security domain is outside TSF control. The active entities may use these resources according to their own security policies but they are not allowed usage of other resources outside their security domain. Therefore the domain description provided in the ARC documentation shall meet TSF access control to the security domain resources as expressed by the SFR and the other SFR must not contradict the security domain definition. If the ARC documentation describes security domains in term of resources not controlled by a SFR, that would mean that a SFR is missing.

In case of composite evaluation the applicative layer could rely upon the underlying platform to correctly instantiate the domains that the TOE defines. The developer should list the used security services offered by the platform to support security domain separation and make reference to these services in the description.

5 SECURE START-UP

The security architecture description shall describe how the TSF initialization process is secure (in accordance with ADV_ARC.1.3C). The information provided in the security architecture description relating to TSF initialisation is directed at the process bringing the TSF from the “down” state (e.g. power-off or after reset) into an initial secure state (i.e. when all parts of the TSF are operational, cf. CEM paragraph 530). For smart cards and similar devices:

- parts of the TSF may be active even in power off e.g. physical protection against undetected manipulation;
- parts of the TSF may be temporally deactivated e.g. in power save modes.

The goal of the secure initialisation process of smart cards and similar devices is to enforce the security objectives even while some TSF parts are not active (i.e. during power off or power save modes) or in activation process (e.g. start-up) or in deactivation process (e.g. transition into power save mode). The secure initialisation process requires that self-protection and non-bypassability is ensured during these transitions. This implies that in any point of time the TOE function is not available if the TSF parts protecting this function are not activated.

The secure initialisation process will be implemented by specific security features or security functionality not directly following SFRs. This specific security functionality and their security mechanisms may be not described in other ADV assurance families. The objective of the ARC documentation for secure initialisation is to provide all the information required to treat these components as part of the TSF.

The secure initialisation process may implement mechanisms protecting the confidentiality or checking the integrity of the implementation of other TSF. Some mechanisms may be not needed after secure initialisation and shall be protected against misuse.

If external interfaces of the initialisation process are fully described as TSFI in terms of actions in ADV_FSP.4 and beyond or the mechanisms as part of the TSF are described in terms of purpose and interactions of modules in ADV_TDS.3 and beyond they do not have to be described again.

6 SELF-PROTECTION

The component ADV_ARC.1.4C requires that the security architecture description demonstrates that the TSF protects itself from tampering.

Self-protection refers to the ability of the TSF to protect itself from manipulation from external entities that may result in changes to the TSF, so that it no longer fulfils the security objectives or SFRs.

Tampering with the TSF may be realized by untrusted active entity running on behalf of an external entity. Mechanisms that provide domain separation to define a TSF domain that is protected from other (user) domains would be identified and described.

Within the Technical Domain of smart cards and similar devices the TOE physical boundaries from which an external entity may intervene are the ports and the surface of the IC. The ports are physical entries of the TOE supporting logical interface that provide access to the TSF for physical parasitic signals. The surface of the chip may be also an entry point for physical parasitic signals. These signals may induce a modification of the stored code & data or of the correct execution of the code.

The functional requirement class FPT (Protection of TSF) contains families of functional requirements that relate to the integrity and management of the mechanisms that constitute the TSF and to the integrity of TSF data. Components from the class FPT are necessary to provide requirements that the SFPs in the TOE cannot be tampered.

Self-protection can therefore not generally be achieved by a mere implementation of an SFR but other security mechanisms may be added and collaborate with the security mechanisms implementing the SFR.

Self-protection of the TSF will be achieved by:

- security mechanisms: the ability of each security mechanism to contribute to the protection against direct attacks;
- binding of security mechanisms: the ability of the security mechanisms to work together in a way that is mutually supportive and provides an integrated and effective whole;
- combination of hardware and software security mechanisms

The initialisation process shall guarantee that the TSF is in an initial secure state and has not been spoofed by any means. The developer shall explain how the initialization process checks the TSF code integrity. The integrity of the initialisation process code shall also be checked during this process.

In some cases the TOE starts up in a low-function mode, a mode whereby untrusted users are able to login and use the services and resources of the TOE. In this mode the code does not run in the evaluated configuration and these services are no more accessible.

In this case the security architecture description shall include an explanation of how the TSF is protected against this code in the evaluated configuration:

- what prevents this code from running;
- what prevents those services from being accessible.

In case of a composite evaluation the platform could provide security services that contribute to the self-protection in cooperation with the application layer security mechanisms. The developer shall list the used security services offered by the platform and make reference to them in the following analysis.

The developer shall describe the security mechanisms and their collaboration to protect the TSF from tampering. The developer shall provide a description on how the TOE reacts in presence of the relevant attacks listed in Annex 7, Application of Attack Potential to Smart Cards and provide a conclusion.

7 NON-BYPASSABILITY

The component ADV_ARC.1.5C requires that the security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality

Non-bypassability is a property that the security functionality as specified by the SFRs is always invoked and cannot be circumvented when appropriate for that specific mechanism (cf. Annex A of CC Part 3).

8 TSF ALWAYS INVOKED

Non-bypassability means firstly that there is no possibility to bypass the SFR-enforcing entity by using unexpected and undocumented paths in the design. Any possibility to bypass the TSF is therefore attributed to a flaw in the design or implementation.

From the EAL4 level, the functional specification shall describe all actions associated with each TSFI (ADV_FSP.4.4C) and the design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules (ADV_TDS.3.9C). In this case all modes or operations of TSFI are documented at a sufficient level to provide evidence of non-bypassability by exploiting a flaw in the design.

Secondly, non-bypassability requires that no Functional Interface can be used to violate the TOE security objectives, to circumvent SFR or to conflict with SFR. When Functional Interfaces exist the developer shall list them and explain either why they have no interaction with the TSF or why they are not providing a path for circumventing the TSF. In this case domain separation description (see the corresponding chapter) may bring evidence of non-bypassability.

Thirdly, non-bypassability deals with those cases where the attacker has only logical access to the TOE as opposed to the case of “tampering” which is to be countered by self-protection (see the corresponding section).

The developer shall describe the security mechanisms and their collaboration to protect the TSF from software attacks exploiting an insufficient design or implementation to meet the TOE security objectives. The developer shall provide a description on how the TOE reacts in presence of the relevant attacks listed in Annex 7, Application of Attack Potential to Smart Cards and provide a conclusion.

9 SIDE CHANNEL

Side channels are unenforced signalling channels carrying information about internal secrets, states or processes provided by monitoring of the processing of any object containing or related to this information (cf. CEM paragraph 1909). The information may be contained in any observable physical value as power consumption of the device, voltage and timing on ports of the output interfaces, electromagnetic emanation on IC surface. The signals of output ports may contain more information than the data intended to be exchange through the logical interface defined in the TSF documentation. The power supply interface and the electromagnetic emanation through the IC surface are not intended for information output at all but may carrying information.

The side channels bypass the TSF because they leak any information intended to be kept secret. The secret information includes but is not limited to authentication reference data (e.g. for PIN verification), symmetric secret or asymmetric private cryptographic keys, timing of data processing enabling other attacks.

The developer shall describe the countermeasures implemented in order to prevent potential side channels of the TOE in the intended operational environment. The side channel analysis as part of the evaluator’s vulnerability analysis shall determine whether side channel exist and are exploitable i.e. these countermeasures are effective.

The developer and the evaluator should consult the SFRs and the security objectives they enforce in order to determine whether an unintended information flow bypass the TSF or not. The implementation of a symmetric message authentication code calculation will keep the confidentiality of the key but it may or may be not required to protect the confidentiality of the processed user data. Therefore the decision about bypass of the TSF by leaking information about the processed user data depends on the security objective enforced by the SFRs.

31. ANNEX 5: CERTIFICATION OF "OPEN" SMART CARD PRODUCTS

PURPOSE

This annex aims at identifying the certification procedure for “open” smart card products in order to guarantee that their changed architecture do not affect the effectiveness of the certified security functionality of a certificate already issued for a different architecture of this product.

PARTICULAR STATUS

None.

CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE

Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS.

1 CONTEXT AND PURPOSE OF THE DOCUMENT

1.1 Definitions

The term product here refers to a generic term that corresponds to a TOE associated to an environment.

The term “platform” refers to the terminology used in Annex 6, COMPOSITE PRODUCT EVALUATION FOR SMART CARDS AND SIMILAR DEVICES about the composition of evaluation results process, applied to the composition evaluation case of an “application on a platform”. Thus, a product designated here as a “platform” is an integrated circuit with a software operating system and sometimes with native applicative code.

An “open platform” is a platform that can host new application after its delivery to the end user (i.e. during the 7th phase of the traditional smartcard lifecycle). Such loadings are called “post-issuance” loading (applications loading after delivery of the smartcard to the end user).

Applications may be installed before the 7th phase, corresponding to “pre-issuance” loading.

A “closed platform” is a platform that cannot host new application after its delivery to the end user.

An “isolating platform” is a platform that maintains the separation of the execution domains of all embedded applications on a platform, as of the platform itself. “Isolation” refers here to domain separation of applications as well as protection of application’s data.

“Architecture” corresponds to the top level structure of the product, namely the ”open platform” with all the applications contained in the product (whenever they are loaded in pre or post issuance).

As the loading of new applications could be considered before or after the evaluation process, the terms “known applications” and “unknown applications” are used to distinguish applications that have been taken into account during the evaluation process from others.

“Known applications” correspond to the original architecture of the certified product. They are all taken into account by the ITSEF during the evaluation process.

“Unknown applications” are applications that were unknown at the time of evaluation. They correspond to an upgrade of the architecture of the evaluated product, from the one stated in the certification report.

1.2 Scope

This annex aims at identifying the certification procedure for open products in order to guarantee that their changed architecture do not affect the effectiveness of the certified security functionality of a certificate already issued for a different architecture of this product. Changed architecture here stands for the addition of applications to the original certified product's architecture (modification of the TOE environment).

Note, that (in contrast to the situation discussed above) a modification of the platform itself will require recertification/assurance continuity of the platform and consequently of the overall product.

In order to take into account, in the certificate, of the changed architecture of these products, the platform shall have some properties, notably isolation properties for applications activated on the product. Indeed, only products that offer these isolation properties ensure that the activation of a new application does not impact the assurance of the functionality as certified. Those platforms which have been evaluated to demonstrate that they offer (under certain constraints) those guarantees are called "open and isolating platform" in this document.

When new applications are loaded on such an open product, verifications of the fulfilment of the platform security constraints by those new applications are required to ensure that the evaluated product (TOE) reaches the AVA_VAN level aimed in its expected IT-environment extended.

Open platforms that do not guarantee isolation of applications are certified as closed platform. Closed platforms that do not authorize post-issuance loading are out of the scope of this document.

1.3 Note's plan

Chapter 2 defines guarantees and constraints on platforms and provides input for evaluation and certification of "open and isolating platforms".

Chapter 3 defines guarantees and constraints on applications and provides input for evaluation of applications on a certified "open and isolating platforms".

2 OPEN AND ISOLATING PLATFORM

2.1 Evaluation

It is referred, in this document, to an open and isolating platform for a platform that has been evaluated in accordance with the elements listed here.

2.1.1 Objectives

2.1.1.1 Analysed functionality

An "open and isolating platform" shall provide the following functionalities that shall be evaluated:

- O1: isolation between all the applications stored on the considered platform, and thus protection against applications that could be hostile;
- O2: protection of the post-issuance loading of applications on the considered platform by verification of the integrity and of the authenticity of the verification of each application, before their activation thanks to the evidences defined in the following OE2.

O1 and O2 shall be objectives for the TOE in the security target of the platform.

2.1.1.2 Evaluation environment

An "open and isolating platform" is a platform which has been submitted to an evaluation process that makes mandatory the following requirements for all the applications that are loaded on the platform:

- OE1: all applications that will be loaded on the platform have to be verified, before their effective installation (activation), according to the constraints imposed by the targeted platform, related to its isolation properties;
- OE2: availability of an integrity evidence for each application to be loaded on the platform (in order to ensure that the loaded application has not been changed since the verification of OE1), and also availability of authenticity evidence of these verifications.

OE1 and OE2 shall be objectives for the environment in the security target of the platform.

OE1 and OE2 are applicable for all applications, whether they will be evaluated to be certified or not. As such, they are applicable for all known or unknown applications.

For known application, the fulfilment of OE1 and OE2 will be verified by the ITSEF. Nevertheless it is still possible to only verify OE1, and describe the way OE2 shall be fulfilled. Then, the ITSEF will verify the fulfilment of OE1 and evaluate the guidance documentation used to fulfil OE2. In such case, the certificate will unambiguously identify these applications and indicate the usage restriction, requiring the final user to apply the guidance documentations to fulfil OE2.

For unknown application, the verification of the fulfilment of OE1 and OE2 is not possible. The platform certificate will consist of certificate usage restriction, requiring the final user to apply the guidance documentation to fulfil OE1 and OE2.

2.1.2 Identification

Speaking generally, certification of open platform should allow the identification of the product evaluated by the ITSEF. This identification consists of:

- the identification of the product in the state in which it has been submitted for evaluation (given to the ITSEF). It includes all the known applications loaded pre-issuance;
- the identification of the all the known applications that can be loaded post-issuance.

Identifiers returned on request by the product shall permit to distinguish the TOE from the product by identifying the platform and listing all the stored applications.

The evaluation shall consider the whole product, whatever the TOE is. Thus, the platform components and the known applications shall be identified in the identification information provided by the security target. This identification information will be specified unambiguously in the certification report of the platform.

The developer shall give to the ITSEF means to verify that the product identifiers available to the ITSEF correspond to a set of components known by the ITSEF (whenever these components belong to the TOE or not).

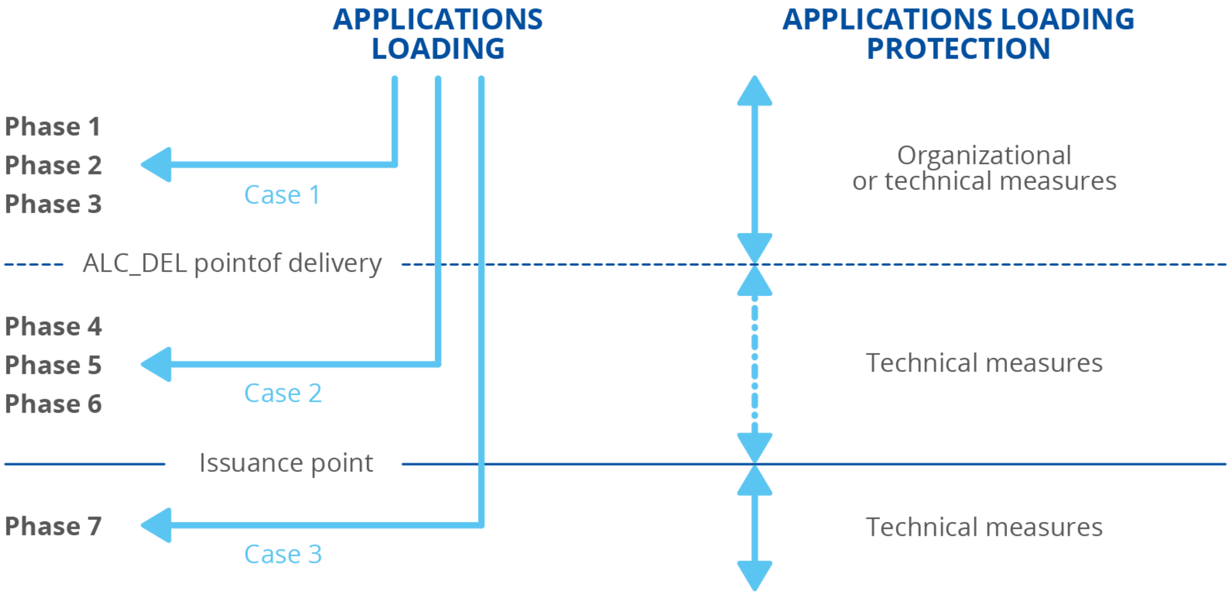
These requirements permit to avoid the risk of certifying products including applications that do not respect the platform constraints, that is to say which may be hostile for the other applications activated on the product.

2.1.3 Life cycle

The following picture shows a phase model of the lifecycle of an open platform. It is just an example of such a life cycle: the ALC delivery point related to the platform evaluation may be different from the one identified here.

Note also that the considered point of delivery can be extended from the one considered in the actual evaluation if the evidence for sites certifications or comparable audit results are provided.

Figure 1: Open and isolating platform life cycle[38].



[38] Note that the phases 1 to 7 are used as defined in the Protection Profile certified under [BSI-CC-PP-0084-2014]: Security IC Platform Protection Profile with Augmentation Packages, https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf

An “open & isolating platform” product may contain pre-issuance and post-issuance applications.

It is useful to precise that the measures to reach the OE2 objective could be of different natures depending of the moment of the loading.

Three different cases may occur:

- Case 1: the application is loaded in pre-issuance and before delivery point ; the OE2 objective may be enforced by organizational measures or technical measures;
- Case 2: the application is loaded in pre-issuance and after the delivery point, organisational measures are not allowed and technical measures must be employed;
- Case 3: the application is loaded in post issuance (after issuance of the product); technical measures associated to OE2 objective must be employed.

By definition all the considered platform allow the case 3 loading (in phase 7 at least).

To precise the way OE1 and OE2 are realised, the security target shall explain the processes implied in the development, in the verification and in the distribution of the application, and the various roles. The security target shall also describe the evaluation scope regarding this detailed lifecycle.

In case known applications are part of the evaluated product the following details of the lifecycle shall also be described in the security target:

- Identification of actors in relation with their role in the management of the processes implied in the application verification;
- Identification of actors in relation with their role in the management of the process implied in the integrity and authenticity protection of applications from their verification to their loading.

In addition, the ALC delivery point may be different between the certified platform and a subsequent composite certification of applications on top of the certified platform (see Section 3). A typical use case might be that the ALC delivery point is moved to a later stage. Thereby, the composite certification would change the classification of phases with respect to whether they belong to Case 1 or Case 2. Platform certification phases of Case 2 could become Case 1 phases of the composite certification, as the point of delivery is postponed, and would then not mandate technical measures. Such a re-classification is accepted and does not contradict nor impact the platform certification.

2.1.4 Product guidance

In relation with the evaluation environment identified in chapter 2.1.1.2, the following specific guidance shall be provided by the developer:

- Application development guidance (in relation with OE1), from which are derived the verification guidance that describe the constraints imposed to the application in order to maintain the isolation property of the platform [ISO_VERIF];
- Application loading protection guidance (in relation with OE2), that correspond to:
    - Organizational measures for application loading [ORG_LOAD] ;
    - Technical measures for application loading that shall describe how to activate the related functionality (corresponding to O2) of the platform, associated to measures necessary to guarantee the authenticity of the verifications (Key protection for example) [TECH_LOAD].

As “open and isolating platforms” always allow the case 3 application loading, [ISO_VERIF] and [TECH_LOAD] have always to be provided by the developer.

It will not be necessary to provide [ORG_LOAD] if the developer does not implement case 1 with organizational measures.

Note that [ISO_VERIF] does not correspond to the guidance mandated by AGD_OPE (guidance documentation for coding of secure applications). [ISO_VERIF] lists all the development rules related to the maintenance of the isolation properties of the platform between applications. Part of AGD_OPE guidance dedicated to the application development lists all the development rules related to application that have to provide specific security properties.

This guidance will have to be evaluated according to AGD or ALC depending of the loading cases considered by the developer.

2.1.5 Evaluated configuration

Depending of the actual lifecycle of the considered product, OE1 and OE2 have to be treated by the ITSEF in the following way:

1) The ITSEF will have to systematically check that all known applications fulfil the OE1 constraint. The ITSEF may rely on developer evidences to check that the application verification has been done. As it cannot be checked for unknown applications, compliance to [ISO_VERIF] will lead to certificate restrictions.
2) When organizational measures are used before the delivery point, the application loading is under developer's responsibility, the associated protection that implements OE2 is covered by ALC Security Assurance Requirement. Therefore, the organizational measures have to be audited.
3) Within the scope of this document, technical measures enforcing OE2 are always used, at least for Case 3. The associated requirements are given in [TECH_LOAD]. Part or all of these requirements can be enforced by ALC Security Assurance Requirements, therefore the corresponding organizational measures have to be audited. Compliance to [TECH_LOAD] that cannot be checked will consist of certificate restriction.

Thus OE1 and OE2 have to be verified for all known applications.

2.2 Open and isolating platform certification

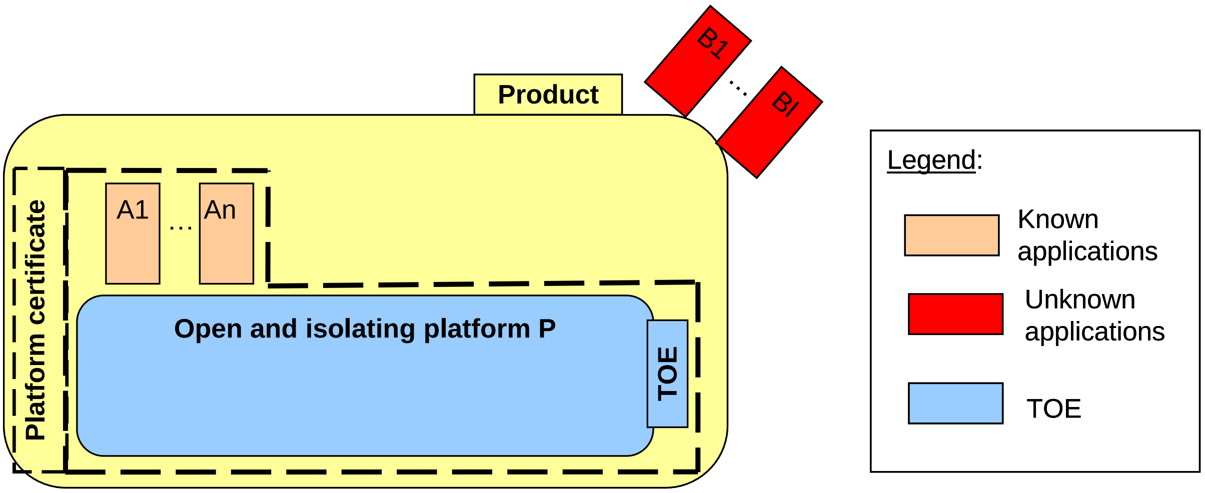
A certification report for an open and isolating platform have the following specificities:

- It will precise that the isolation of applications, and also the protection of post-issuance application loading have been studied in order to identify that this platform is conformant to the concept of "open and isolating platform". The "evaluated configuration chapter" will precise that the evaluated product is an "open and isolating platform".
- It will identify, in the "architecture" and "evaluated configuration" chapters, all the known applications that have been checked by the ITSEF during the evaluation process. It will also precise that all the identified applications in the certification report have been checked according to the OE1 and OE2 objectives.
- The "evaluated configuration" chapters will also precise that products constituted of a subset of known applications are also certified.
- The "usage restrictions" chapter shall state the constraints OE1 and OE2 and the references to the guidance [ISO_VERIF], [ORG_LOAD] and [TECH_LOAD], which apply to any application loaded in the product, in particular any new application unknown at evaluation time. Note that this chapter may also contain usage restrictions that are not linked to the open and isolation properties of the platform.
- It will describe in the "product life cycle" chapter, the different type of application loading applicable to the product and considered by the developer.
- It may contain as well the list of known application for which OE1 only has been verified. In such cases, the certificate will unambiguously identify these applications and indicate the usage restriction, requiring the final user to apply the guidance documentations to fulfil OE2.

The loading of unknown applications as Bi (i $\in$ [1,l]) implies that the product no more fully suits the product's architecture stated in the open and isolating platform certificate. The evaluation results are only valid if all the other applications loaded on the platform respect the platform certification constraints. Thus the resulting product architecture which respects the security constraints of the associated certificates can be considered as certified. It is up to the risk manager to rely on the assurance of verification of OE1 and OE2 provided by the actor in charge of the deployment of these applications or to rely on the schema. In this last case (if the CC schema solution is selected), a maintenance as stated in chapter 2.3 hereafter will have to be performed.

The following picture shows the certified product. Here the TOE only corresponds to the platform. Ai (i $\in$ [1,n]) applications correspond to known pre-issuance applications and are then identified in the platform certification report.

Figure 2: Product related to an open and isolating platform TOE



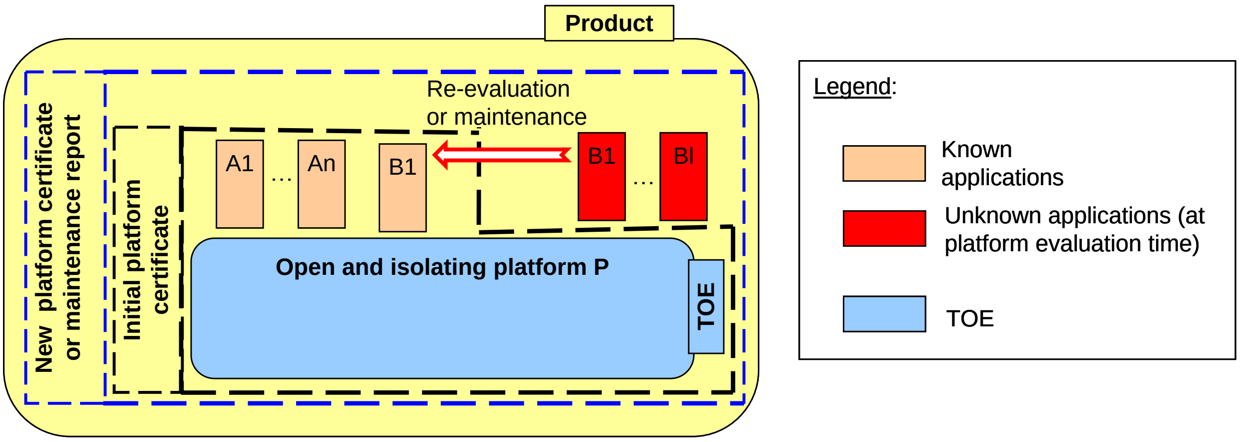
2.3 Open and isolating platform maintenance

The assurance continuity process can be applied to open and isolating platform certificates like to any other certificate. This chapter only deals with the specificities of this process for open and isolating platform when no major change of the platform has been performed, and when the developer wants the certified product to include some applications that where unknown during the initial evaluation.

The certificate restrictions concerning these new applications must be checked. When the verification and loading of these new applications are done in the same previously evaluated way than for the known applications, thus responding to OE1 and OE2, a maintenance report can be issued if the site visit report is still valid.

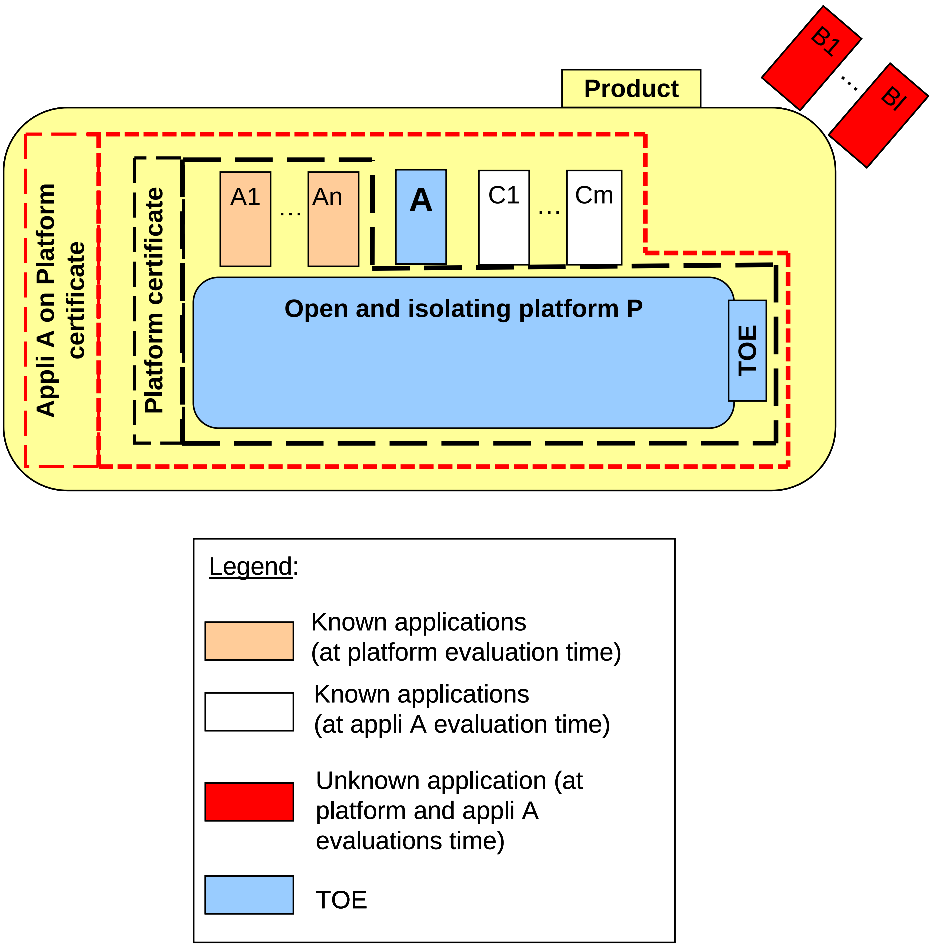
The developer will have to provide the evidences related to those new applications with its impact analysis (same type of evidences than those provided during the initial evaluation process for applications Ai (i ∊ [1,n])). The impact analysis shall also describe the main functionality of the new applications (applications Bi (i ∊ [1,l])).

Figure 3: Maintained product related to an open and isolating platform TOE.



3 APPLICATIONS ON AN OPEN AND ISOLATING PLATFORM

Figure 4: Standard certificate TOE and related product.


Product
B1
…
Bl
Appli A on Platform certificate
Platform certificate
A1
…
An
A
C1
…
Cm
Open and isolating platform P
TOE
Legend:
Known applications (at platform evaluation time)
Known applications (at appli A evaluation time)
Unknown application (at platform and appli A evaluations time)
TOE

In this picture, platform P and applications Ai (i ∊ [1,n]) have been evaluated and have led to an open and isolating platform certificate. All Ai applications are identified in the platform certificate.

Applications A and Cj (j ∊ [1,m]) correspond to application loaded after the platform certification but known at application evaluation time. They might either correspond to post (case 3) or pre-issuance (case 1 or 2) applications.

Application A is the application targeted by the application on platform evaluation. We consider here that this evaluation is done according to the composition process defined in Annex 6 with reference to:

- the usual security application development guidance for applications that provide security functionality;
- the guide [ISO_VERIF] that describes the constraints imposed to the applications in order to maintain the isolation property;
- and possibly the application loading protection guidance [ORG_LOAD] or [TECH_LOAD].

So the considered TOE here is the “application A on platform P”. Of course other specific CC activities will have to be performed by the ITSEF. This chapter only focus on the requirements imposed by the open and isolating platform evaluation.

3.1 Evaluation

3.1.1 Objectives from the platform certificate

The standard evaluation process requires considering all the known applications. The applications Ai have already been considered at platform evaluation and are identified in the platform certificate report (see 2.2). So in the resulting

A on P certification report all the new known applications Cj have to be identified according to the rules defined in 2.1.1.2.

To precise the way OE1 and OE2 are realised, the security target shall detail actors implied in the development, in the verification and in the distribution of the applications, and their roles. The security target should also describe the evaluation scope regarding this detailed lifecycle.

The ITSEF will have to check that all applications respect the platform requirements OE1 and OE2 and that all applications Ai and Cj fulfil the security functional compatibility constraints of application A (see chapter 3.1.2).

For the applications Cj the respect of the requirements OE1 and OE2 shall be evaluated following the same rules than for the known applications Ai at platform evaluation time (see paragraph 2.1.5), with reference to platform guidance (see paragraph 2.1.4).

For the targeted application A the respect of the two requirements OE1 and OE2 shall be realised during the composition activities (see assurance requirements ADV_COMP of Annex 6) and may follow the rules defined in 2.1.5 with reference to platform guidance defined in 2.1.4 as for the Cj applications.

The loading of unknown applications as Bk (k ∊ [1,m]) implies that the product no more fully suit the product's architecture stated in the open and isolating platform certificate of A on P. The evaluation results are only valid if all the other applications loaded on the platform respect the platform certification constraints. The product's architectures which respect the security constraints of the associated certificates can be considered as certified. It is up to the risk manager to rely on the assurance of verification of OE1 and OE2 provided by the actor in charge of the deployment of these applications or to rely on the schema. In this last case, the sponsor will then ask for maintenance as stated in chapter 3.3 hereafter.

3.1.2 Applications security functional compatibility

The targeted A application may require the respect by the co-existing applications of some specific security constraints (for instance, an e-passport application cannot coexist with an application that allows the transmission of the user identity without its agreement) that are explicitly described in the application A guide AGD_OPE.

Pre-requisite: The main functionality of application loaded pre-issuance (applications Ai (i ∊ [1,n])) shall be described in the ETR and ETR-COMP related to the platform evaluation.

The ITSEF will have to check that functionalities of applications Cj and Ai fulfil the security constraint required by application A.

If only some specific product architectures could be certified, regarding the functional compatibility analysis, the ITSEF shall mention it to the developer and ask him to provide each of these architectures.

3.2 Certification

All coexisting applications with the certified one are identified in such a certification report as in an open and isolating platform (see 2.2). But the "evaluated configuration" chapter of the certification report will precise that products constituted of a subset of known applications are also certified.

3.3 Maintenance of certificates for applications on open and isolating platform

In case the developer wants the certified product to include as well some unknown applications such as Bk, the necessary certificate restrictions concerning these applications must be established.

A Impact Analysis Report (IAR) may be provided:

- when the verification and loading of these applications is done in the same way than for the known applications Ai or Cj, thus responding to OE1 and OE2 requirements;
- there is no functional compatibility constraints required by the certified A application.

The developer will have to provide the evidences related to those new applications loading with its impact analysis (same type of evidences than those provided during the initial evaluation process for application Ai or Cj). The impact analysis shall also describe the main functionality of the new applications Bk.

If this loading is made according to organisational measures, the certification body will be able to directly maintain the certificate, according to the conditions defined in Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATE, if the site visit report is still valid.

32. ANNEX 6: COMPOSITE PRODUCT EVALUATION FOR SMART CARDS AND SIMILAR DEVICES

PURPOSE

This annex defines concept and methodology applicable to composite product evaluation. The product consists of a hardware part and associated libraries (if applicable) and a software part which is embedded in the hardware and is built to operate with this hardware. Both parts can be evaluated independently; thus, the efficiency of evaluation could increase as the hardware part can be used with many different software applications

PARTICULAR STATUS

None.

CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE

Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS.

1 INTRODUCTION

1.1 Background

The Common Criteria (CC) are being widely used for smart card products security evaluation. Smart card evaluation showed very early a need for interpretation and supporting documents.

The initial reason was that a smart card is built up with a combination of two parts: a hardware integrated circuit (IC) part and a software part often developed by different actors with specific objectives.

Another reason is that the software part may be layered itself consisting of an “Operating System layer” with possibly integrated applicative functions and an “Application layer” on top of it that may contain different applications. All these software parts can be developed by different actors with specific objectives.

One objective was to independently perform one evaluation of a platform to address several applications and customers.

Another objective was to create one or several applications to load on one or several certified platforms.

The objective for Application Integration was to install one or several applications onto one already certified platform to reduce the evaluation effort keeping a high level of confidence.

To achieve these objectives, a transfer of knowledge and a reuse of evidence have been defined.

1.2 Definitions

The hardware part with associated libraries (if applicable) is evaluated independently as it can be used with many different software applications.

The software is embedded in the hardware and is built to operate with this hardware. The resulting product is the one which is used in the field (cellular phones, banking cards, health cards, identity, digital signature, e-pass, e-ticketing etc.) and on which customers/users need to gain confidence.

Software applications may be built to operate with the support of an OS. The OS provides a separation mechanism between itself and the software applications as well as services to the software applications.

Another specificity of the smart card type product is that the software part has to use, control, configure or activate the security mechanisms provided by the hardware. And the software applications may use, control, configure or activate the security mechanisms provided by the OS.

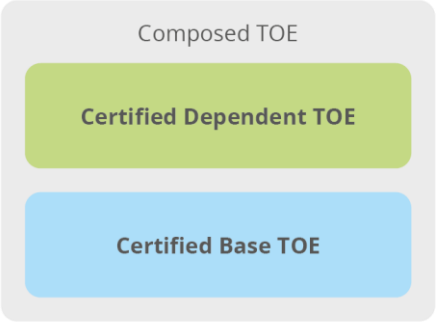
1.3 Composite product evaluation and ACO

Although the CC introduce the specific assurance class ACO for composition, this class is not suitable for usual smart card and similar devices evaluation.

ACO addresses a TOE composed of two certified TOEs: the Base TOE and the Dependent TOE (see Figure 1). The evaluation of the composed TOE consists in evaluating the interaction between both TOEs, reusing evaluation results of Base TOE and Dependent TOE.

The result of this evaluation is not an EAL level, but a CAP level which is not comparable to an EAL level. Furthermore, ACO class is applicable up to Extended-Basic assurance level, whereas smart cards especially in banking or signature type application require 'High Level' assurance.

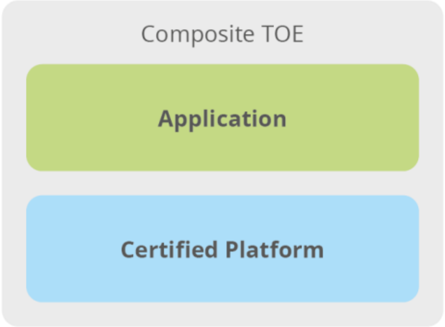
Figure 1: ACO composed TOE (package CAP)



For smart card and similar devices the composite product is the final product for which an EAL level certification is required. This allows a direct comparison with similar products certified after a single evaluation.

Considering smart card architecture, it is composed of a hardware platform typically an integrated circuit and embedded software layer on top of the hardware platform. The embedded software may be itself an Application or is composed itself of an "OS layer" with a further "Application layer" on top of the „OS layer"". The hardware and maybe the "OS layer" together may form a Platform with an Application on top of it. In the Composite TOE evaluation, the Platform is certified, the Application is evaluated and the results of the Platform Certification are reused. See for Figure 2 security certification of the entire Composite TOE.

Figure 2: Composite product evaluation (current approach)



The hardware platform properties related to security and security functionality are provided in the security target. The platform provides mechanisms to protect the composite product assets, but the composite product behaviour depends widely on the software application having to use, to configure and activate these security mechanisms.

The OS platform offers security services and provides mechanisms to protect the composite product assets. The composite product behaviour depends widely on the software application having to use the security services and to use, to configure and activate these services. Therefore, the platform evaluation results provide security recommendations and conditions formulated in the platform user guidance for the software application implementation.

The composite product evaluator shall examine amongst other that the combination of application and platform does not lead to any exploitable vulnerability. The smart card composite evaluation methodology defines precise work units with clear statement on the information needed from the platform developer and provides an agreed "framework" for information transfer from platform to composite product evaluator.

The information required is already available from the platform evaluation tasks and no additional work is required from platform developer.

- There is no need for details on the platform development class ADV.
- The user guidance (AGD) of the platform is considered early in the development of the composite product and provides all interfaces information needed.
- The development and the evaluation of the composite TOE rely on the proper implementation of the evaluated interfaces of the platform.
- The proper use of all relevant interfaces between platform and application is in the scope of the composite product evaluation.
- Test (ATE) and vulnerability assessment (AVA) are performed on the composite product taking advantage of platform evaluation results.

The concept of the Composite TOE evaluation does not limit the composite evaluation in EAL and resistance against attacks, i.e. up to 'high', whereas Composed TOE (CAP package) is limited by resistance against attacks 'extended-basic'.

1.4 Objective and scope

The objective of this annex is to precisely define tasks for the different parties involved in the Composite TOE evaluation.

The aim is not to define an additional assurance class, but to define refinements to the existing assurance requirements for a composite product evaluation.

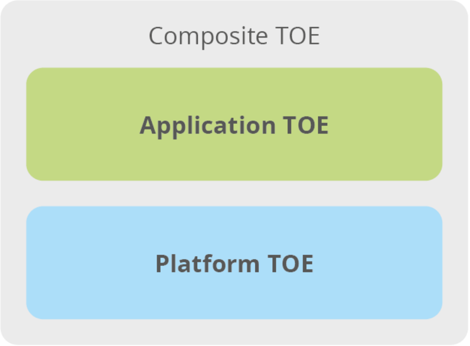
This annex addresses TOEs that are of the type belonging to the technical domain "Smartcards and Similar Devices". However, this annex is not restricted to smart cards and similar devices only and can be applied in principle (possibly with adequate adaptations, as far as necessary) for any other secure ICT product where an independently evaluated component is part of a final composite product to be evaluated.

The smart cards and similar devices technical domain is defined as: related to smart cards and similar devices where significant portions of the required security functionality depend upon hardware features at a chip level (for example smart card hardware/ICs, smart card composite products, TPMs (Trusted Platform Modules) used in trusted computing, digital tachograph cards, etc.).

2 DEFINITIONS / TERMINOLOGY

2.1 Definitions

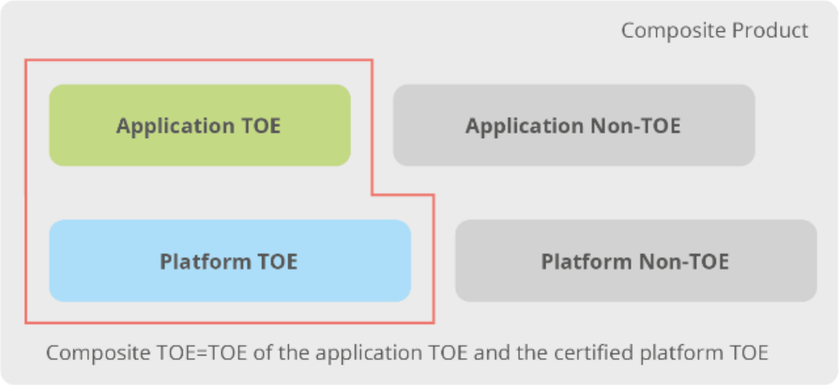
Figure 3: Composite Product



The Composite TOE is a TOE that is composed of a superposition of 2 layers as depicted in Figure 3, the initial layer (identified as the ‘Platform’) and the supplementary layer (the ‘Application’):

- The initial layer is the underlying layer that could be either a single product, or a composite product. We consider that this layer has been already certified.
- The supplementary layer is dependent on the platform. This layer is subject to the composite evaluation.

Figure 4: Composite TOE



The composite TOE is a composition between the platform and the application, and is composed of the ‘platform TOE’ and the ‘application TOE’ as marked in the red box in Figure 4, with the following restrictions:

- The application TOE cannot rely on platform functionalities that are outside the platform TOE, in the Non-TOE parts. This is depicted in grey layer ‘Non-(platform) TOE’ in Figure 4.
- The composite TOE is composed with a superset of the entire application TOE, and a superset of the minimum platform TOE functionalities required for the correct execution of the composite product.
- The non-TOE subset of the application can use platform TOE functionalities. As usual, the composite evaluation needs to determine that this non-TOE application part is non-interfering with the application TOE – neither directly nor through the usage of the platform functionalities.

Exemplifying, this may be an operating system (‘application’) running on a hardware platform (‘underlying platform’) or a Java Card^{TM} applet (‘application’) running on a Java Card runtime environment (‘platform’).

Several composition steps can follow each other i.e. a composite product may rely on a platform which is itself a composite product. For such compositions with a previously composed product the same rules apply.

These definitions comply with ACO class definitions where:

- A platform is the base component,
- An application is the dependent component.

2.2 Roles

The following roles shall be considered in the composite evaluation activities:

- Platform Developer: Entity developing the platform; it might also be the applicant of the platform evaluation.
- Platform Evaluator: Entity performing the platform evaluation.
- Platform Certification Body: Entity performing the platform certification, defined in CC terminology as evaluation authority.
- Application Developer: Entity developing the application running on the platform.
- Composite Product Integrator: Entity installing the applications on the platform.
- Composite Product Evaluator: Entity performing the composite product evaluation.
- Composite Product Certification Body: Entity performing the composite product certification defined in CC terminology as evaluation authority.
- Composite Product Evaluation Applicant: Entity in charge of contracting the composite product evaluation (it might be the Application Developer).

Each evaluation shall associate particular organizations or persons to these generic roles.

In order to illustrate the role of the Composite Product Integrator, here are some examples:

- Native Smart cards: The ‘underlying platform’ is an integrated circuit and the Platform Developer is the integrated circuit (chip) manufacturer; the ‘application’ is a card operating system and its application(s) and the Application Developer is the developer of the smart card software and the application(s). In this case, the role of the Composite Product Integrator is played by (i) the chip manufacturer embedding the core of the operating system into the ROM of the chip, then by (ii) the card manufacturer usually loading some parts of the operating system and the applications into NV-Memories (EEPROM and/or Flash) of the chip.
- Java Card technology-enabled devices: The ‘underlying platform’ is the Java Card runtime Environment (Java Card RE) on chip and the Platform Developer is the card manufacturer/issuer; the ‘application’ is the Java Card applet and may be developed by the Application Developer. In this case, another role is the Composite Product Integrator who may be played by the domain/application service provider or by a trust centre loading the applet and often personalizing the card electronically.

3 COMPOSITE EVALUATION CONCEPT

3.1 What are the issues?

The assets to be protected are the final composite product assets defined in the composite product Security Target.

The security mechanisms involved in the protection of these assets are those provided by the platform and by the application itself.

Some of the security mechanisms and security services provided by the platform may require configuration, programming or activation by the application.

Therefore the Application Developer needs all the information (in form of a guidance or user’s manual) related to the platform security mechanisms and security services the application has to manage.

Furthermore he needs the platform security target in order to build the composite product security target and to ensure consistency of security definition between platform and application development. Evaluation is performed and validated on the final composite product.

If the Platform and the Application parts are combined in a composite product the Composite Product Evaluator has to examine, that the level of security required by the Security Target is achieved. Therefore the Composite Product Evaluator has to execute the evaluation tasks needed with respect to the Security Target of the final composite product and to provide the related ETR. In this perspective, the Composite Product Evaluator should reuse the platform evaluation and certification results thus saving cost and time.

3.2 What information is needed?

The Composite Product Evaluator does not need all platform evaluation results. The security certificate and the certification report ensure that the platform has been evaluated according to the Common Criteria. The Composite Product Evaluator will need complementary information on the assurance measures where platform and application development interfere. To check that the application meets the security requirements of the platform usage, the Composite Product Evaluator will need the same level of knowledge about the platform as the Application Developer. In addition to the standard amount of evaluation contributions according to the assurance package chosen for the composite evaluation (e.g. an EAL level) evaluation, the following is needed (see section 4.7 ‘Deliveries’ for further details):

- All the information delivered from the Platform Developer to the Composite Product Integrator,
- All the information delivered from the Platform Developer to the Application Developer,
- ETR for composite evaluation prepared by the Platform Evaluator, see chapter 5 ‘ETR for composite evaluation’ (including information about vulnerability analysis and penetration testing),
- Information on compliance of the Security Targets and the designs of the platform and the application prepared by the Application Developer,
- Information on compliance of the delivery procedures of the Platform and Application Developers with the acceptance procedure of the Composite Product Integrator,
- Information on integration of both parts using their correct certified versions and the correct configuration parameters. This information shall be prepared by the Composite Product Integrator; it also implies assurance that the application is correctly managed by the Platform Developer (e.g. in the case of smart card where ROM code is supplied for masking on the platform).

Composite Product Certification Body will need the same amount of information as the Composite Product Evaluator.

3.3 Case of composite product change

In case of composite product changes due to a minor change of the platform or the application or both, please refer to Annex 11, ASSURANCE CONTINUITY.

If a change comes from the platform, the assessment of the change for the platform is given by the Platform Certification Body. On this basis, the assessment of the change for the composite product is given by the Composite Product Certification Body.

If a change comes from the application, the assessment of the change for the composite product is given by the Composite Product Certification Body.

3.4 Specific case when the application is already certified

In the case where both platform and application have already been certified, a partial evaluation work may be performed regarding the results already obtained from previous application evaluation. Nevertheless, the composite evaluation tasks as defined in this document are still required.

4 COMPOSITE EVALUATION ACTIVITIES DESCRIPTION

The current approach can be applied independent of the evaluation assurance level (EAL) for the composite product aimed. Where some evaluation activities are not applicable due to the EAL chosen, they are also not expected to be applied.

For the following paragraphs, one can assume that the level of assurance of the platform is equivalent or higher compared to the composite product evaluation level.

Other cases must be discussed within the schemes.

The composite-specific developer and evaluator action elements as well as the evaluator actions (work units) belonging to the composition activities are defined as the refinements for composite evaluation, see Appendix 1: Composite-specific requirements.

4.1 Evaluation of the composite product Security Target

A Security Target for the composite product has to be written and evaluated.

The Composite Product Evaluator has to examine that the Security Target of the composite product[39] does not contradict the Security Target of the underlying platform[40]. In particular, it means that the Composite Product Evaluator has to examine the Composite- and the Platform- Security Target for any conflicting assumptions, compatibility of security objectives, security requirements and security functionality needed by the application.

[R1] This task can be reduced, if some matching has been checked for Protection Profiles claimed by each Security Target.

[R2] The Composite Product Evaluation Applicant must ensure that the security target of the platform is available to the Application Developer, to the Composite Product Evaluator and to the Composite Product Certification Body. The information available in public version of the security target may not be sufficient.

4.2 Integration of the application in the configuration management system

[R3] The Composite Product Evaluator shall verify that the evaluated version of the application has been installed onto / embedded into the evaluated version of the underlying platform.

[R4] The Composite Product Evaluation Applicant must ensure that appropriate evidence generated by the Composite Product Integrator is available to the Composite Product Evaluator. This evidence may include, amongst other, the configuration list of the Platform Developer provided within its acknowledgement statement.

4.3 Compatibility check for delivery and acceptance procedures

[R5] The Composite Product Evaluator shall verify that delivery procedures of the Application and Platform Developers are compatible with the acceptance procedure used by the Composite Product Integrator.

[39] Hereinafter referred to as Composite-ST.
[40] Hereinafter referred to as Platform-ST.

[R6] The Composite Product Evaluator shall verify that all configuration parameters prescribed by the Application and Platform Developers (e.g. pre-personalization data, pre-personalisation scripts) are used by the Composite Product Integrator.

[R7] The Composite Product Evaluation Applicant must ensure that appropriate evidence generated by the Composite Product Integrator is available to the Composite Product Evaluator. This evidence may include, amongst other: Element of evidence for the application reception, acceptance and parameterisation by the Platform Developer (in form of acknowledgement statement).

4.4 Compliance of designs

[R8] The Composite Product Evaluator shall verify that stipulations for the Application Developer imposed by the Platform Developer in its certified user guidance and referenced in the platform certification report are fulfilled by the composite product, i.e. have been taken into account by the Application Developer.

[R9] The Composite Product Evaluation Applicant must ensure that the following are made available to the Composite Product Evaluator:

- The platform-related user guidance,
- ETR for Composition prepared by the Platform Evaluator, see chapter 5 ‘ETR for composite evaluation’,
- The Certification Report for the platform prepared by the Platform Certification Body,
- A rationale for secure composite product implementation including evidence prepared by the Application Developer.

4.5 Composite product functional testing

[R10] Some application functionality testing can only be performed on emulators, before its embedding/integration onto the platform, as effectiveness of this testing (pass/fail) may not be visible using the interfaces of the composite product. Nevertheless, functional testing of the composite product shall be performed also on composite product samples according to description of the security functions of the Composite TOE and using the standard approach as required by the relevant assurance class. No additional developer’s action is required here.

[R11] Since the amount, the coverage and the depth of the functional tests of the platform have already been validated by the platform certificate, it is not necessary to re-perform these tasks in the composite evaluation. Please note that ETR for Composition (see chapter 5 ‘ETR for composite evaluation’) does not provide any information on functional testing for the platform.

[R12] The Composite Product Evaluation Applicant must ensure that the following is available to the Composite Product Evaluator:

-Composite product samples suitable for testing.

4.6 Composite product vulnerability analysis

[R13] The Composite Product Evaluator shall perform a vulnerability analysis for the composite product using, amongst other, the results of the platform evaluation and certification. This vulnerability analysis shall be confirmed by penetration testing.

[R14] The Composite Product Evaluator has to check that the confidentiality protection of the embedded software in memory of the platform is consistent with the confidentiality level claimed by the Application Developer for ALC_DVS.

[R15] In special cases, the vulnerability analysis and the definition of attacks might be difficult, need considerable time and require extensive pre-testing, if only documentation is available. The platform may also be used in a way that was not foreseen by the Platform Developer and Platform Evaluator, or the Application Developer may not have followed the stipulations provided with the platform certification. Different possibilities exist to shorten composite vulnerability analysis in such cases:

- The Composite Product Evaluator can consult the Platform Evaluator and draw on his experience gained during the platform evaluation.
- Separation of vulnerabilities of application and platform with the use of “open samples” (“open samples” are samples of the platform on which the Composite Product Evaluator can load software on his own discretion). The intention is to use test software without the application countermeasures without deactivating any platform inherent countermeasure. The aim is clearly not to repeat the platform evaluation. (See Annex 7, APPLICATION OF ATTACK POTENTIAL TO SMARTCARDS AND SIMILAR DEVICES for further details).

[R16] The Composite Product Evaluation Applicant must ensure that the following are made available to the Composite Product Evaluator:

- The ETR for Composition (ETR_COMP) prepared by the Platform Evaluator, see chapter 5 'ETR for composite evaluation' below,
- The Certification Report for the platform prepared by the Platform Certification Body.

4.7 Deliveries

The tables below summarize the documentation deliveries that are exchanged between parties to enable the composite evaluation activities as defined in the previous paragraphs.

The Composite Product Evaluation Applicant is in charge of the initialization of the process.

The Composite Product Evaluation Applicant is responsible for maintaining or creating any Non-Disclosure Agreement (NDA) that would be necessary between all the parties involved in the composition activities.

The Non-Disclosure Agreement should be established according to the sensitivity and ownership of the information to be exchanged.

Table 1: Definition of composition documents

Nr	Document / Contribution	Description
1	**Platform Security Target**	Security Target of the platform as referenced in the platform certification report.
2	**Platform open samples for testing**	Platform samples as defined in Annex 7.
3	**Platform user guidance**	It encompasses all platform user guidance and manuals needed for the Application Developer and the Composite Product Integrator being referenced in the platform certification report.
4	**Platform ETR_COMP**	ETR for composition as defined in chapter 5 and referenced in the platform certification report.
5	**Platform certification report**	Platform certification report issued by authorized Platform Certification Body.
6	**Design compliance evidence**	It enfolds evidence elements on how the requirements on the application design, imposed by the platform's guidance and certification report, are fulfilled in the composite product. If such a requirement was not followed, a rationale that the chosen composite product implementation is still secure shall be given here.
7	**Composite configuration evidence**	It comprises: (i) Identification elements of the composite product - proving that the correct, certified version of the platform is used in the composite product, - proving that the correct, evaluated version of the application has been integrated; and (ii) Evidence elements that security measures prescribed by the Platform and Application Developers are actually being applied by the Composite Product Integrator.
8	**Delivery and acceptance procedures evidence**	Evidence elements how the delivery procedures of the Platform and Application Developers are compatible with the acceptance procedure of the Composite Product Integrator.

The following table shows which documents/contributions of Table 1 shall be provided to which actor within the composite evaluation process.

Table 2: Main Deliveries between actors

##	Document / Contribution	Composite product evaluation Applicant	Composite product Integrator	Application Developer	Composite product Evaluator	Composite product CB
1	**Platform Security Target**	No	No	Yes	Yes	Yes
2	**Platform open samples for testing**	No	No	No	Yes	Yes
3	**Platform user guidance**	No	Yes	Yes	Yes	Yes
4	**Platform ETR_COMP**	No	No	No	Yes	Yes
5	**Platform certification report**	Yes	Yes	Yes	Yes	Yes
6	**Design compliance evidence**	No	No	No	Yes	Yes
7	**Composite configuration evidence**	No	No	No	Yes	Yes
8	**Delivery and acceptance procedures evidence**	No	No	No	Yes	Yes

The next table shows some example of Composite TOE use cases with definition of the components and the roles.

Table 3: Example of composite TOE use cases

Components & roles definitions	**Smartcard – I** The Composite TOE is built of - a Security IC with an application code loaded in ROM (Masking operation) and application data loaded in EEPROM	**Smartcard – II** The Composite TOE is built of - a Security IC without ROM, but offering Flash technology and Flash loader - an application code and data loaded into the flash by a smart Card manufacturer	**Java Card** The Composite TOE is built of - a Java Card Platform - a Java card application: the applet
The Platform is	The Security IC	The Security IC with the Flash memory and the Flash Loader	The Java Card Platform including Card Manager with Applet loader facility
The Application is	The Operating System code plus additional data files	The Operating System code, Flash memory initialization data and application data	The Applet
The Platform Developer is	The Security IC Manufacturer: - Develops and manufactures the Security IC	The Security IC Manufacturer: - Develops, manufactures and delivers the Security IC with Flash technology to the Composite Product Integrator	The Java Card Platform developer: - Develops the Java Card with applet loading mechanism to the Composite Product Integrator.

The Application Developer is	The Smartcard Software developer: - Develops the application; - Provides the application to Composite product integrator	The Smartcard Software developer: - Develops the application; - Delivers the application to the Composite Product Integrator	The Applet developer: - Develops the applet; - Delivers the applet to the Composite Product Integrator
The Composite Product Integrator is	The Security IC Manufacturer: - is in charge of OS masking in ROM and of loading Application data in EEPROM; - Delivers the Composite TOE to be evaluated	The Card Manufacturer: - is in charge of loading the application into the flash using Security IC flash loader; - Delivers the Composite TOE to be evaluated	The Card Issuer: - Loads the applet on the Java Card platform using applet loading mechanism; - Delivers the Composite TOE to be evaluated

5 ETR FOR COMPOSITE EVALUATION

5.1 Objective of the document

A standard Evaluation Technical Report (ETR) contains proprietary information that cannot be made public. The ETR for composite evaluation (ETR_COMP) document is compiled from the ETR in order to provide sufficient information for composite product evaluation with a certified platform. The information that is presented in the ETR_COMP document shall be a subset of the information presented in the full ETR. It should enable the Composite Product Evaluator and the respective Certification Body to understand the considered attack paths, the performed tests and the effectiveness of countermeasures implemented by the platform.

A template for an ETR_COMP document is given in Appendix 2: ETR for composite evaluation template.

5.2 Generic rules:

[R17] The ETR for composite evaluation should be produced by the Platform Evaluator based on the platform evaluation results. This task should be considered when determining the evaluation work program to reduce additional cost and effort.

[R18] The content of ETR_COMP has to strike the right balance between protecting platform developer's and/or Platform Evaluator's proprietary information and providing sufficient information for the Composite Product Evaluator and the respective Certification Body, cf. Table 2 above.

[R19] ETR_COMP shall not include information affecting national security.

[R20] The information provided must be approved by all parties involved in the platform evaluation (i.e. the Evaluator, the Certification Body, the developer and applicant of the evaluation). The platform Certification Body shall validate its consistency with the original ETR. The platform certification report shall reference the ETR for composite evaluation.

[R21] If the current ETR_COMP itself relies on a composite evaluation, and if there is direct interface with the previous platform, the reference to this previous composite evaluation ETR_COMP must be supplied.

[R22] The ETR_COMP is not meant to include copies of information from other available platform evidence, as the Security Target and Guidance. However, the composite evaluation is much supported by references to the relevant sections.

5.3 Exchange of the ETR for Composition

An ETR_COMP contains intellectual property of the Platform Developer as well as of the Platform Evaluator, and also the Platform Certification Body has a role in its content. At the minimum the document should be considered restricted. The ETR_COMP document is created and maintained by the Platform Evaluator. However, at a given certification the Platform developer is the point of contact for the Application Developer.

The application developer will contact the Platform Developer for delivery of the ETR_COMP to the point of contact at the Composite Product Evaluator. The Platform Developer will check its confidentiality management rules (existence of relevant NDA with Lab and CB, etc.) whether delivery is possible. If necessary the platform developer will contact the Platform Certification Body about the intent of the delivery of the ETR_COMP.

Next the Platform Developer will contact the Platform Evaluator to request the delivery (using a secure method and only marked versions will be distributed) of the ETR_COMP to the given contact point of the Composite Product Evaluator. If the OK is granted, either the Platform Evaluator or the Platform Developer will send the ETR_COMP to the Composite Product Evaluator depending on the agreements between these two parities.

Depending on (contractual) agreement between the Platform Developer and Platform Evaluator, there may be deviations from the described procedure of delivery of the ETR_COMP to the Composite Product Evaluator.

If necessary the Platform Evaluator and the Composite Product Evaluator will exchange more detailed information. This is always under control of the Platform Developer. In case of clarification the Platform Evaluator and the Composite Product Evaluator will be the main parties. If an additional assurance statement is required then also the Platform certification body will be involved in the exchange.

5.4 Content of the ETR for composite evaluation

[R23] The information required is focused on:

1) Formal information about the platform like its exact identification, reference to the certification report etc.
2) Information about the Platform design.
3) Information about the evaluated configuration of the Platform.
4) Information on delivery procedures, involved sites and data exchange.
5) Information about penetration testing of the Platform including the considered attack paths and summary of test results.
6) Information about penetration testing of the supporting functions in the platform
7) Observations and recommendations for users.

5.4.1 Formal information

[R24] This section of ETR_COMP shall provide formal information on the platform evaluation as:

- product identification,
- applicant and developer identities,
- identities of the evaluation facility and the certification body,
- assurance level of the evaluation,
- formal evaluation and certification results like pass/fail,
- references to the ETR.

5.4.2 Platform design

[R25] This section of ETR_COMP shall provide a high-level description of the IT product and its major components based on the deliverables required by the assurance class ADV of the Common Criteria. The intent of this section is to characterize the degree of architectural separation of the major components and to show possible technical dependencies between the platform and an application using the platform (e.g. dependencies between HW platform and SW application). This shall include an outline of security mechanisms of the platform covered by the platform evaluation.

5.4.3 Evaluated configuration

[R26] This section of ETR_COMP shall provide information about the evaluated configuration of the Platform based on the developer’s configuration list or relevant parts as needed or on a case by case basis. The platform must unambiguously be identifiable and this identification shall be commensurate with the evaluated configuration as stated in the platform certification report.

[R27] If applicable, generation and installation parameter settings being security relevant for the Platform should be explained and their effect on the defence against attacks is outlined (e.g. key length, counters limits). This includes methods for the application developer and evaluator to verify the values of these settings, in order to verify that the expected evaluated configuration is used.

[R28] This evidence may include TOE installation, generation and start-up procedures as outlined in AGD_PRE to enforce that the platform is configured in a secure manner.

5.4.4 Delivery procedures, sites and data exchange

[R29] For supporting composite evaluation, evaluation evidence can be necessary for delivery of the platform, and acceptance procedures of the application and related data to be integrated during development and production. Therefore, evaluation evidence about AGD_PRE and ALC_DEL + AGD_PRE might be relevant.

[R30] The ETR_COMP shall provide an overview of the sites involved in the development and production of the platform, including the role of each site and the date of latest site visit.

[R31] For the composite evaluation, of an OS on an IC the description of phase 1 and 4 are needed and will be detailed in this document. The delivery of the IC dedicated software and guidance to the application developer should also be considered. In addition details on the fab-key protection mechanism should be identified.

For an IC as per Annex 3, APPLICATION OF CC TO INTEGRATED CIRCUITS, the deliveries under consideration are:

1) The delivery of the embedded application code to the microcontroller manufacturer, (in case of Flash products this may be replaced by the delivery of a key from the microcontroller manufacturer to the developer of the Security IC Embedded Software)
2) The delivery of the microcontroller to the entity in charge of the next step (testing, embedding into micro-module, card manufacturing).

For an OS the deliveries under consideration are:

1) The delivery of the embedded application code to the manufacturer (if the code will be embedded in ROM) or product integrator (if the code will be embedded in EEPROM or Flash).
2) The delivery of the smart card/platform (IC with embedded OS) to the in charge of the next step (product integrator, personaliser, etc.)
3) The delivery of security guidance
4) The exchange of key-material for access to the smart card/platform (IC with embedded OS).

5.4.5 Penetration Testing

[R32] This section of ETR_COMP shall provide information about the independent vulnerability analysis performed by the Platform Evaluator with the attack scenarios having been considered, the penetration testing having been performed and the reference to the corresponding rating (quotation) of the attack potential (following the Annex 7] valid at the time of the platform certification).

[R33] Information about penetration testing results should include:

- details necessary for understanding the attack scenarios/paths
- the assessments of penetration results as well as a summary showing that all attack methods as outlined in Annex 11 were addressed during the vulnerability analysis.

If a potential vulnerability has to be resolved by adhering to guidance this must be clear from the summary including a reference to a specific section in guidance or if possible a guidance element.

[R34] The attack scenario descriptions should provide sufficient details to support the Composite Product Evaluator to reproduce attacks, which require additional countermeasures in the Composite TOE.

[R35] In accordance with the requirements of CEM, this information is available within the ETR. So it can be compiled for ETR_COMP.

[R36] This section shall also mention the rating of access to ‘open samples’ (i.e. public/restricted/sensitive/critical). The use of ‘open samples’ shall be considered in the assessment of the attack path. Please note that ‘open samples’ are evaluation tools, but do not represent a TOE.

5.4.6 Observations and recommendations

[R37] The evaluated user guidance documentation shall contain all information required to use the TOE in a secure way as defined in the platform security target including recommendations on how to avoid residual vulnerabilities and unexpected behaviour. The recommendations and the user guidance documentation shall be consistent. The Platform Evaluator shall verify that the ETR for Composition only contains recommendations on the secure use that are also addressed as requirements in the user guidance. The user guidance requirements must be specific enabling the Application Developer to perform design compliance analysis

[R38] However, in specific cases detailed information might be required in addition to the guidance documents such as:

- Observations on the evaluation results (e.g. specific TOE configuration for the evaluation),
- Recommendations/stipulations for the Composite Product Evaluator: specific information on use of the evaluation results (e.g. about specific testing necessary during a composition evaluation).

Any such observation or recommendation/stipulation may come from the Platform Evaluator and the Platform Certification Body.

6 EVALUATION/CERTIFICATION REPORTS AND PLATFORM CERTIFICATE VALIDITY

[R39] Results of a composite evaluation shall be provided to the Composite Product Certification Body in form of an Evaluation Technical Report for the composite product. This Composite Product ETR shall contain, amongst others, the final overall verdict for the composite evaluation based on the partial verdicts for each assurance component being in scope of the current composite evaluation. There shall be a reference to this CC supporting document in the Composite Product ETR and the Composite Product Certification Report.

[R40] As the composite product certificate covers also the platform, the composite product certificate validity is linked to the validity of the platform certificate.

[R41] The Composite Product Certification Body needs an up-to-date certificate or an assessment from the Platform Certification Body on the status of the platform certificate in question.

[R42] As a general rule the Composite Product Certification Body will ask for a reassessment of the platform if the date of the platform's ETR for Composition is more than one and a half year before the submission of the report containing the full results of the composition penetration tests. This reassessment consists of either a re-evaluation of the platform focussing on a renewal of the vulnerability analysis (surveillance task) or alternatively, a confirmation statement of the Platform Certification Body may be requested.

[R43] Note that in the case the entire composite product is set up as a chain of composite products constructed on top of each other (e.g. the platform itself is already a composite product) the maximum validity period of 18 months is related to the eldest ETR for Composition used in this chain of composite products. In addition, dependencies from a lower level ETR for Composition to a higher level ETR for Composition need to be considered when reusing the results in the composite evaluation on top.

[R44] Note also that if the platform's ETR for Composition was issued less than a year and a half ago before submission of the related composite evaluation tasks, but there was a major change in the state of the art in performing relevant attacks on the platform (e.g. a major change in the "Application of Attack Potential to Smart Cards" Annex7, or a major change in attack methods or attack ratings) then the Composite Product Certification Body has the right to require a reassessment focusing on the new attack method.

[R45] Validity and relevance of the platform certificate for the current composite product certification shall be acknowledged by the Composite Product Certification Body and includes the determination of equivalence of single assurance components (and, hence, of assurance levels) belonging to different CC versions, if the platform certification was according to another CC version than the current composite certification is. Such equivalence shall be established / acknowledged by the Composite Product Certification Body.

[R46] The Composite Product Certification Body can issue a security certificate for the composite product, if:

- the verdicts for the Composite Product ETR is PASS, and
- validity and topicality of the platform certificate for the current composite product are acknowledged by the Composite Product Certification Body.

[R47] Note that, if the Composite Product Evaluator detects some failures resulting from Platform testing (e.g. vulnerabilities due to improved attack methods or techniques), the results shall be communicated to the Composite Product Certification Body. The Composite Product Certification Body shall then take appropriate steps together with the Platform Certification Body, e.g. to invoke a re-assessment or re-certification of the platform TOE.

[R48] The Platform Certification Body shall verify that the recommendations in the ETR for composition of the platform are consistent with the requirements provided in the platform user guidance before issuing the certification report. When inconsistencies are detected the Platform Certification Body has the freedom to add missing information for the Application Developer in the certification report.

APPENDIX 1: COMPOSITE-SPECIFIC REQUIREMENTS

In the following, the Composite-specific developer and evaluator action elements as well as the evaluator actions (work units) belonging to the composition activities (cf. chapter 4 above) are defined. They require the evidence elements as listed in section 4.7.

These refinements to the assurance requirements aim to give the Composite Product Evaluator and Application developer a precise guidance on which relevant aspects have to be described and assessed in the context of a composite evaluation and the tasks to be performed.

It allows the Composite Product Certification Body to check using the composite product ETR that the required (mandatory) tasks have properly been performed.

All composite-specific evaluator actions have to be documented according to the scheme rules and finalised by one of the verdicts PASS, FAIL or INCONCLUSIVE. As these actions are refinements of the traditional actions focused on the composition activities, these verdicts have to be integrated to the overall verdict.

This approach can be applied independently of the aimed evaluation assurance level (EAL) for the composite product. Where some evaluation activities are not applicable due to the EAL chosen, the related composite-specific tasks are also not expected to be applied.

For convenience of composite-specific activities and associated work units identification, each refinement is named as *_COMP, where * is the name of the assurance class it is related to.

Appendix 1.1 Composite-specific tasks for a composite evaluation in CC

Consistency of composite product Security Target (ASE_COMP)
The composite-specific work units defined in this chapter are intended to be integrated as refinements to the evaluation activities of the ASE class listed in the following table. The other activities of ASE class do not require composite-specific work units.

CC assurance family	Evaluation activity	Evaluation work unit	Composite-specific work unit
ASE_OBJ	ASE_OBJ.2.1C ASE_OBJ.2.1C ASE_OBJ.2.3C	ASE_OBJ.2-1 ASE_OBJ.2-1 ASE_OBJ.2-3	ASE_COMP.1-5 ASE_COMP.1-6 ASE_COMP.1-6
ASE_REQ	ASE_REQ.1.6C ASE_REQ.2.9C ASE_REQ.1.6C ASE_REQ.2.9C ASE_REQ.2.8C ASE_REQ.2.3C	ASE_REQ.1-10 ASE_REQ.2-13 ASE_REQ.1-10 ASE_REQ.2-13 ASE_REQ.2-12 ASE_REQ.2-4	ASE_COMP.1-1 ASE_COMP.1-1 ASE_COMP.1-2 ASE_COMP.1-2 ASE_COMP.1-3 ASE_COMP.1-4

ASE_COMP.1 Consistency of Security Target

Objectives

The aim of this activity is to determine whether the Security Target of the composite product[41] does not contradict the Security Target of the underlying platform[42].

Application notes

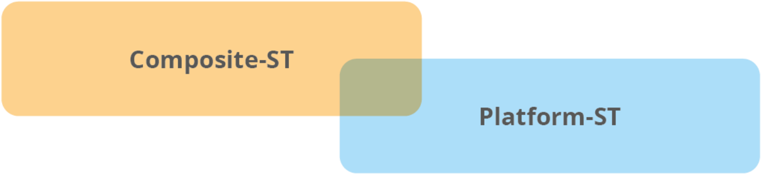
These application notes aid the developer to create as well as the evaluator to analyse a composite Security Target and describe a general methodology for it. For detailed information / guidance please refer to the single work units below.

In order to create a composite Security Target the developer should perform the following steps:

Step 1: The developer formulates a preliminary Security Target for the composite product (the Composite-ST) using the standard code of practice. The Composite-ST can be formulated independently of the Security Target of the underlying platform (Platform-ST) – at least as long as there are no formal PP conformance claims.

[41] Hereinafter referred to as Composite-ST.
[42] Hereinafter referred to as Platform-ST. Generally, a Security Target expresses a security policy for the TOE defined.

Step 2: The developer determines the overlap between Platform-ST and Composite-ST through analysing and comparing their TOE Security Functionality (TSF)[43][44]:



Step 3: The developer determines under which conditions he can trust in and rely on the Platform-TSF being used by the Composite-ST without a new examination.

Having undertaken these steps the developer completes the preliminary Security Target for the composite product.

It is not mandatory that the platform and the composite TOE are being certified according to same version of the CC. It is due to the fact that the application can rely on some security services of the platform, if (i) the assurance level of the platform covers the intended assurance level of the composite TOE and (ii) the platform security certificate is valid and up-to-date. Equivalence of single assurance components (and, hence, of assurance levels) belonging to different CC versions shall be established / acknowledged by the Composite Product Certification Body, cf. chapter 6.

If a PP conformance is claimed (e.g. composite ST claim conformance to a PP that claims conformance to a hardware PP), the consistency check can be reduced to the elements of the Security Target having not already been covered by these Protection Profiles. The fact of compliance to a PP is not sufficient to avoid inconsistencies. Assume the following situation, where → stands for “complies with”
Composite-ST → SW PP → HW PP ← platform-ST
The SW PP may require any kind of conformance [45], but this does not change the ‘additional elements’ that the platform-ST may introduce to the HW PP. In conclusion, these additions are not necessarily consistent with the composite-ST/SW PP additions: There is no scenario that ensures the consistency ‘by construction’.

Note that consistency may not be direct matching: e.g. objectives for the platform environment may become objectives for the composite TOE.

Dependencies:

No dependencies.

Developer action elements:

ASE_COMP.1.1D

The developer shall provide a statement of compatibility between the Composite Security Target and the Platform Security Target. This statement can be provided within the Composite Product Security Target.

Content and presentation of evidence elements:

ASE_COMP.1.1C

The statement of compatibility shall describe the separation of the Platform-TSF into relevant Platform-TSF being used by the Composite-ST and others.

ASE_COMP.1.2C

The statement of compatibility between the Composite Security Target and the Platform Security Target shall show (e.g. in form of a mapping) that the Security Targets of the composite product and of the underlying platform match, i.e. that there is no conflict between security environments, security objectives, and security requirements of the Composite Security Target and the Platform Security Target. It can be provided by indicating of the concerned elements directly in the Security Target for the composite product followed by explanatory text, if necessary.

[43] Because the TSF enforce the Security Target (together with organisational measures enforcing security objectives for the operational environment of the TOE).
[44] The comparison shall be performed on the abstraction level of SFRs. If the developer defined security functionality groups (TSF-groups) in the TSS part of his Security Target, the evaluator should also consider them in order to get a better understanding for the context of the security services offered by the TOE.
[45] e.g. “strict” or “demonstrable” according to the CC.

Evaluator action elements:

ASE_COMP.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Evaluator actions:

Action ASE_COMP.1.1E

ASE_COMP.1.1C

ASE_COMP.1-1 The evaluator shall check that the statement of compatibility describes the separation of the Platform-TSF into relevant Platform-TSF being used by the Composite-ST and others.

Note that TSF means 'TOE Security Functionality' in CC V3, whereby the TSF content is represented by SFRs. The respective TOE summary specification (TSS) shall provide, for each SFR, a description on how each SFR is met[46]. The evaluator shall use this description in order to understand the contextual frame of the SFRs.

If the developer defined security functionality groups (TSF-groups) in the TSS part of his Security Target as such contextual frame of the SFRs, the evaluator should also consider them in order to get a better understanding for the context of the security services offered by the TOE.

This work unit relates to the Step 2 of the Application Notes above. In order to determine the intersection area the evaluator considers the list of the Platform-SFRs (given in the ST of the underlying platform) as single properties of the platform's security services.

To give an example, let assume that there are the following Platform-SFRs: Cryptographic operations FCS_COP.1/RSA, FCS_COP.1/AES, FCS_COP.1/EC as well as tamper-resistance FPT_PHP.3 and limited capabilities and availability FMT_LIM.1 and FMT_LIM.2[47].

These Platform-SFRs shall be separated in three groups:

- IP_SFR: Irrelevant Platform-SFRs not being used by the Composite-ST.
- RP_SFR-SERV: Relevant Platform-SFRs being used by the Composite-ST to implement a security service with associated TSFI.
- RP_SFR-MECH: Relevant Platform-SFRs being used by the Composite-ST because of its security properties providing protection against attacks to the TOE as a whole and are addressed in ADV_ARC. These required security properties are a result of the security mechanisms and services that are implemented in the Platform TOE.

The second and third group RP_SFR-SERV and RP_SFR-MECH exactly represent the intersection area in question. For example, IP_SFR = {FCS_COP.1/AES}, RP_SFR-SERV= {FCS_COP.1/RSA, FCS_COP.1/EC } and RP_SFR-MECH = { FPT_PHP.3, FMT_LIM.1, FMT_LIM.2}, i.e. AES is not used by the composite TOE, but all other Platform-SFRs are used. However, the RP_SFR-MECH cannot be directly connected to SFRs in the Composite-ST.

The size of the overlapping area (i.e. the content of the group RP_SFR-SERV and RP_SFR-MECH) results from the concrete properties of the Platform-ST and the Composite-ST. If the Composite-ST does not use any property of the Platform-ST and, hence, the intersection area is an empty set (RP_SFR-MECH ∪ RP_SFR-SERV) = {∅}), no further composite evaluation activities are necessary at all: In such a case there is a technical, but not a security composition.

The result of this work unit shall be integrated to the result of ASE_REQ.1.6C/ ASE_REQ.1-10 (or the equivalent higher components if a higher assurance level is selected) and ASE_REQ.2.9C/ ASE_REQ.2-13.

ASE_COMP.1-2 The evaluator shall examine the statement of compatibility to determine that the Platform-TSF being used by the Composite-ST is complete and consistent for the current composite TOE.

In order to determine the completeness of the list of the Platform-TSF being used by the Composite-ST, the evaluator shall verify that:

- Platform-SFR = IP_SFR ∪ RP_SFR-SERV ∪ RP-SFR-MECH

[46] cf. CC Part 3, ASE_TSS.1.1C.
[47] FMT_LIM.1 and FMT_LIM.2 can be found in BSI-CC-PP-0084-2014, Security IC Platform Protection Profile with Augmentation Packages.

- Elements that belong to RP_SFR-SERV and RP-SFR-MECH are taken into account during the evaluation of the composite TOE. The IP-SFR are obviously part of the Platform-TOE but they are not considered during the evaluation of the composite TOE.

In order to determine the consistency of the list of the Platform-TSF being used by the Composite-ST, the evaluator shall verify that there are no ambiguities and contradictory statements.

More details on the consistency analysis can be found in common CC documents.

The result of this work unit shall be integrated to the result of ASE_REQ.1.6C/ ASE_REQ.1-10 (or the equivalent higher components if a higher assurance level is selected) and ASE_REQ.2.9C/ ASE_REQ.2-13.

ASE_COMP.1.2C

ASE_COMP.1-3 The evaluator shall check that the security assurance requirements of the composite evaluation represent a subset of the security assurance requirements of the underlying platform.

This work unit relates to the Step 2 of the Application Notes above. In order to ensure a sufficient degree of trustworthiness of the Platform-TSF the evaluator compares the TOE security assurance requirements (SARs) of the composite evaluation with those of the underlying platform. The evaluator decides that the degree of trustworthiness of the Platform-TSF is sufficient, if the Composite-SAR represent a subset of the Platform-SAR:

Platform-SAR $\supseteq$ Composite-SAR,

e.g. the EAL chosen for the composite evaluation does not exceed the EAL applied to the evaluation of the platform.

The result of this work unit shall be integrated to the result of ASE_REQ.2.8C/ ASE_REQ.2-12.

ASE_COMP.1-4 The evaluator shall examine the statement of compatibility to determine that all performed operations on the relevant TOE security functional requirements of the platform are appropriate for the Composite-ST.

This work unit relates to Step 3 of the Application Notes above. The relevant TOE security functional requirements of the platform comprise at least the elements of the group RP_SFR-SERV (cf. the work unit ASE_COMP.1-1) but also the RP-SFR-MECH may be presented as relevant TOE security functional requirements. The non-relevant TOE security functional requirements belong to IP_SFR.

In order to perform this work unit the evaluator compares single parameters of the relevant SFRs of the platform with those of the composite evaluation. For example, the evaluator compares the properties of the respective components FCS_COP.1/RSA and determines that the Composite-ST requires a key length of 2048 bit and the Platform-ST enforces the RSA-function with a key length of 1024 and 2048 bit, i.e. this parameter of the platform is appropriate for the Composite-ST. Note, that the Composite-SFRs need not necessarily be the same as the Platform-SFRs, e.g. a trusted channel (FTP_ITC.1) in the composite product can be built using an RSA implementation (FCS_COP.1/RSA) of the platform.

The result of this work unit shall be integrated to the result of ASE_REQ.2.3C/ ASE_REQ.2-4.

ASE_COMP.1-5 The evaluator shall examine the statement of compatibility to determine that the relevant TOE security objectives of the Platform-ST are not contradictory to those of the Composite-ST.

This work unit relates to Step 3 of the Application Notes above. The relevant TOE security objectives of the Platform-ST are those that are mapped to the relevant SFRs of the Platform-ST (cf. the work unit ASE_COMP.1-1).

In order to perform this work unit the evaluator compares the relevant TOE security objectives of the Platform-ST with those of the Composite-ST and determines whether they are not contradictory.

The result of this work unit shall be integrated to the result of ASE_OBJ.2.1C/ ASE_OBJ.2-1.

ASE_COMP.1-6 The evaluator shall examine the statement of compatibility to determine that the significant security objectives for the operational environments of the Platform-ST are not contradictory to those of the Composite-ST.

This work unit relates to Step 3 of the Application Notes above. In order to determine which assumptions of the Platform-ST are significant for the Composite-ST the evaluator analyses the objectives for the environment of the Platform-ST and their separation in the following groups:

- IrOE: The objectives for the environment being not relevant for the Composite-ST, e.g. the objectives for the environment about the developing and manufacturing phases of the platform.

- CfPOE: The objectives for the environment being fulfilled by the Composite-ST automatically. Such objectives of the environment of the Platform-ST can always be assigned to the TOE security objectives of the Composite-ST. Due to this fact they will be fulfilled either by the Composite-SFR or by the Composite-SAR automatically. To give an example, let there be an Objective for the environment OE.Resp-Appl of the Platform-ST: 'All User Data are owned by Smartcard Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Smartcard Embedded Software as defined for the specific application context' and a TOE security objective OT.Key_Secrecy of the Composite-ST: 'The secrecy of the signature private key used for signature generation is reasonably assured against attacks with a high attack potential.' If the private key is the only sensitive data element, then the Objective for the environment OE.Resp-Appl is covered by the TOE security objective OT.Key_Secrecy automatically.
- SgOE: The remaining Objectives for the environment of the Platform-ST belonging neither to the group IrOE nor CfOE Exactly this group makes up the significant objectives for the environment for the Composite-ST, which shall be addressed in the Composite-ST.

In order to accomplish this work unit the evaluator compares the significant security objectives for the operational environment of the Platform-ST with those of the Composite-ST and determines whether they are not contradictory. If necessary, the significant security objectives for the operational environment of the Platform-ST shall be included into the Composite-ST including the related assumptions from which the objectives for the environment are drawn. The inclusion is not necessary, if the Composite-ST already contains equivalent (or similar) security objectives (covering all relevant aspects) and assumptions.

Since assurance of the development and manufacturing environment of the platform is confirmed by the platform certificate, the respective platform-objectives, if any, belong to the group IrOE

Assurance of development and manufacturing environment is usually completely addressed by the assurance class ALC, and, hence, requires no explicit security objective.

The result of this work unit shall be integrated to the result of ASE_OBJ.2.1C/ ASE_OBJ.2-1 and ASE_OBJ.2.3C/ ASE_OBJ.2-3.

Integration of composition parts and consistency check of delivery procedures (ALC_COMP)
The composite-specific work units defined in this chapter are intended to be integrated as refinements to the evaluation activities of the ALC class listed in the following table. The other activities of ALC class do not require composite-specific work units.

CC assurance family	Evaluation activity	Evaluation work unit	Composite-specific work unit
ALC_CMS	ALC_CMS.1.2C	ALC_CMS.1-2	ALC_COMP.1-1
AGD_PRE	AGD_PRE.1.1C	AGD_PRE.1-1	ALC_COMP.1-2
ALC_CMC	ALC_CMC.4.8C	ALC_CMC.4-10	ALC_CMC.4-10

NB: If the level of the assurance requirement chosen is higher than those identified in this table, the composite-specific work unit is also applicable.

ALC_COMP.1 Integration of the application into the underlying platform and Consistency check for delivery and acceptance procedures

Objectives

The aims of this activity are to determine whether

- the correct version of the application is installed onto/into the correct version of the underlying platform, and
- the preparative guidance procedures of Platform and Application Developers are compatible with the acceptance procedure of the Composite Product Integrator.

Dependencies:

No dependencies.

Developer action elements:

ALC_COMP.1.1D

The developer shall provide components configuration evidence; cf. item #7, item #8 and item #3 in Table 1, section 4.7.

Content and presentation of evidence elements:

ALC_COMP.1.1C

The components configuration evidence shall show that the evaluated version of the application has been installed onto / embedded into the certified version of the underlying platform

ALC_COMP.1.2C

The components configuration evidence shall show that:

i. The evidence for delivery and acceptance compatibility shall show that the delivery procedures of the Platform and Application Developers are compatible with the acceptance procedure of the Composite Product Integrator.
ii. the evidence shall show that preparative guidance procedures prescribed by the Platform and Application Developers are either actually being used by the Composite Product Integrator or compatible with the Composite Product Integrator guidance and do not contradict each other

Evaluator action elements:

ALC_COMP.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_COMP.1.2E

The evaluator shall confirm that the evidence for delivery compatibility is complete, coherent, and internally consistent.

Evaluator actions:

Action ALC_COMP.1.1E

ALC_COMP.1-1 The evaluator shall examine the evidence that the evaluated version of the application has been installed onto / embedded into the correct, certified version of the underlying platform.

The AGD_PRE documentation of the platform provided by the platform developer contains requirements for the secure acceptance of the platform and security measures to which the application developer or product composite integrator has to adhere. The application developer has to provide evidence that (if applicable), these requirements are followed up and the required security measures are implemented.

The special composite evaluator activity is to check the evidence of the version correctness for both parts of the composite product and that the secure acceptance and installation of the platform has been performed.

For the underlying platform, the evaluator shall determine that the actual identification of the platform is commensurate with the respective data in the platform certificate as part of following up on the procedures as specified in the AGD_PRE of the platform.

For the application, the relevant task is trivial due to the fact that the Composite Product Evaluator has to perform this task in the context of the assurance family ALC_CMS.

Components identification evidence can be supplied in two different ways: technical and organisational. A technical evidence of version correctness is being generated by the composite product itself: the platform and the application return – in each case – strings containing unambiguous version numbers as answers to the respective commands. E.g. it can be the return string of a command or the hard copy of the Windows-Information (like ‘About’); in case of smart cards it can be an appropriate ATR.

A technical evidence of version correctness for hardware can also be supplied, if applicable, by reading off the unambiguous inscription on its surface. Note that there are no physical indication existing on most smart cards microcontrollers.

Technical evidence is recommended to be provided.

An organisational evidence of version correctness is being generated by the Composite Product Integrator on the basis of his configuration lists containing unambiguous version information of the platform and the application having been composed into the final composite product.

For example, in case of smart cards it can be an acknowledgement statement (e.g. configuration list) of the integrated circuit[48] manufacturer to the embedded software[49] manufacturer containing the evidence for the versions of the chip, the embedded software and its pre-personalisation parameters[50].

Organisational evidence is always possible and, hence, shall be provided.

The result of this work unit shall be integrated to the result of ALC_CMS1.1C/ ALC_CMS.1-2 (or the equivalent higher components if a higher assurance level is selected).

ALC_COMP.1-2 The evaluator shall examine the acceptance procedure of the Composite Product Integrator, the delivery procedures of the Application Developer and the Platform developer to see that they are compatible and where necessary either applied by the Composite Product Integrator or prescribed in the preparative guidance. .

The general information of the preparative guidance requirements that amongst others includes configuration parameters is represented and has to be examined in the context of the assurance family AGD_PRE [1.2C]. The special evaluator activity is to examine the developer's evidence and to decide whether the Composite Product Integrator appropriately treats this special subset of the preparative guidance requirements.

The evaluator has to examine this provided evidence which includes the check whether the delivery procedures of the Platform and Application Developers are compatible with the acceptance procedure of the Composite Product Integrator.

In the cases where the Composite Product Integrator leaves preparative guidance requirements prescribed by the Platform Developer and Application Developer to the user, the Composite Evaluator verifies that such requirements are presented in the preparative guidance of the Composite evaluation.

For example, for a Java Card as Composite TOE, the Card Issuer has to set all parameters as prescribed by the Java Card Platform and the Applet Developers while installing the applet onto the Java Card platform; cf. Table 3, section 4.7. And And also verify that the package is byte code verified and has a valid digital signature.

The result of this work unit shall be integrated to the result of AGD_PRE.1.2C/AGD_PRE.1-4 and ALC_CMC.4.8C/ ALC_CMC.4-10.

Composite design compliance (ADV_COMP)

The composite-specific work units defined in this chapter are intended to be integrated as refinements to the evaluation activities of the ADV class listed in the following table. The other activities of ADV class do not require composite-specific work units.

CC assurance family	Evaluation activity	Evaluation work unit	Composite-specific work unit
ADV_ARC	ADV_ARC.1.1E	ADV_ARC.1.1C/ ADV_ARC.1-1	ADV_COMP.1-1
ADV_IMP	ADV_IMP.1.1E	ADV_IMP.1.1C/ ADV_IMP.1-1	ADV_COMP.1-1
ADV_TDS	ADV_TDS.1.2E	ADV_TDS.1-7	ADV_COMP.1-1

NB: If the level of the assurance requirement chosen is higher than those identified in this table, the composite-specific work unit is also applicable.

[48] -> underlying platform

[49] -> application

[50] Any data supplied by the embedded software manufacturer that is injected into the non-volatile memory by the integrated circuits manufacturer. These data are for instance used for traceability and/or to secure shipment between phases (cf. [Smartcard IC Platform Protection Profile with augmentation packages, Version 1.0, January 2014, registration number BSI PP 084-2014], sec. 7.7).

ADV_COMP.1 Design compliance with the platform certification report, guidance and ETR_COMP

Objectives

The aim of this activity is to determine whether the requirements on the application, imposed by the underlying platform, are fulfilled in the composite product.

Application notes

The requirements on the application, imposed by the underlying platform, can be formulated in the relevant certification report (e.g. in form of constraints and recommendations), user guidance and ETR_COMP (in form of observations and recommendations) for the platform. The developer of the composite product shall regard each of these sources, if available (cf. Table 2, section 4.7), and implement the composite product in such a way that the applicable requirements are fulfilled.

The TSF of the composite product is represented at various levels of abstraction in the families of the development class ADV. Experiential, the appropriate levels of design representation for examining, whether the requirements of the platform are fulfilled by the composite product, are the TOE design (ADV_TDS), security architecture (ADV_ARC) and the implementation (ADV_IMP). In case, these design representation levels are not available (e.g. due to the assurance package chosen is EAL1), the current activity is not applicable (see the next paragraph for the reason).

Due to the definition of the composite TOE (cf. section 2.1 ‘Definitions’) the interface between the underlying platform and the application is the internal one, hence, a functional specification (ADV_FSP) as representation level is not appropriate for analysing the design compliance.

Security architecture ADV_ARC as assurance family is dedicated to ensure that integrative security services like domain separation, self-protection and non-bypassability properly work. It is impossible and not the sense of the composite evaluation to have an insight into the architectural internals of the underlying platform (it is a matter of the platform evaluation). What the Composite Evaluator has to do in the context of ADV_ARC is

(i) to determine whether the application uses services of the underlying platform within its own Composite-ST to provide domain separation, self-protection, non-bypassability and protected start-up; if no, there is no further composite activities for ADV_ARC; if yes, then

(ii) the evaluator has to determine, whether the application uses these platform-services in an appropriate/secure way (please refer to the platform user guidance, cf. item #3 in Table 1, section 4.7).

Since consistency of the composite product security policy has already been considered in the context of the Security Target in the assurance family ASE_COMP (see page 31 above), there is no necessity to consider non-contradictoriness of the security policy model (ADV_SPM) of the composite TOE and the security policy model of the underlying platform.

Dependencies:

No dependencies.

Developer action elements:

ADV_COMP.1.1D

The developer shall provide a design compliance justification; cf. item #6 as well as items #3, #4, #5 in Table 1, section 4.7.

Content and presentation of evidence elements:

ADV_COMP.1.1C

The design compliance justification shall provide a rationale for design compliance – on an appropriate representation level – of how the requirements on the application, imposed by the underlying platform, are fulfilled in the composite product.

Evaluator action elements:

ADV_COMP.1.1E

The evaluator shall confirm that the rationale for design compliance is complete, coherent, and internally consistent.

Evaluator actions:

Action ADV_COMP.1.1E

ADV_COMP.1-1 The evaluator shall examine the rationale for design compliance to determine that all applicable requirements on the application, imposed by the underlying platform, are fulfilled by the composite product.

In order to perform this work unit the evaluator shall use the rationale for design compliance as well as the TSF representation on the ADV_TDS, ADV_ARC and ADV_IMP levels on the one side and the input of the platform developer in form of the certification report, guidance and ETR_COMP on the other side. The evaluator shall analyse which platform requirements are applicable for the current composite product, based on the identified RP-SFR-MECH and RP-SFR-SERV. The evaluator shall compare each of the applicable requirements with the actual specification and/or implementation of the composite product and determine, for each requirement, whether it is fulfilled. As result, the evaluator confirms or disproves the rationale for design compliance.

For example, platform guidance may require the application to perform a special start-up sequence testing the current state of the platform and initialising its self-protection mechanisms. Such information might be found in the description of secure architecture ADV_ARC of the composite TOE; see also the Application Note above.

A second example, platform guidance may require the application to perform a DFA check on the DES operation, while the application is implementing BAC in an e-passport MRTD [PP-0055[51]]. The ADV_ARC will explain whether the platform guidance is followed up or not, and in case that the requirements in the platform guidance are not followed a corresponding reasoning will be provided. The arguments of the developer explain why a non-compliancy will not introduce vulnerabilities.

The appropriate representation level (ADV_TDS, ADV_ARC and/or ADV_IMP), what the analysis is being performed on, can be chosen and mixed flexibly depending on the concrete composite TOE and the requirement in question. Where it is not self-explaining, the evaluator shall justify why the representation level chosen is appropriate.

The evaluator activities in the context of this work unit can be spread over different single evaluation aspects (e.g. over ADV_TDS and ADV_IMP). In this case the evaluator performs the partial activity in the context of the corresponding single evaluation aspect. Then the notation for this work unit shall be ADV_COMP.1-1-TDS, ADV_COMP.1-1-ARC and ADV_COMP.1-1-IMP, respectively.

If the assurance package chosen does not contain the families ADV_TDS, ADV_ARC or ADV_IMP (e.g. EAL1), this work unit is not applicable (cf. Application Note above).

The result of this work unit shall be integrated to the result of ADV_TDS.1−2E/ ADV_TDS.1-7, ADV_ARC.1.1E/ ADV_ARC.1.1C/ ADV_ARC.1-1, ADV_IMP.1.1E/ ADV_IMP.1.1C/ ADV_IMP.1-1 (or the equivalent higher components if a higher assurance level is selected).

Composite functional testing (ATE_COMP)

The composite-specific work units defined in this chapter are intended to be integrated as refinements to the evaluation activities of the ATE class listed in the following table. The other activities of ATE class do not require composite-specific work units.

CC assurance family	Evaluation activity	Evaluation work unit	Composite-specific work unit
ATE_COV	ATE_COV.1.1C	ATE_COV.1-1	ATE_COMP.1-1
ATE_FUN	ATE_FUN.1.2C	ATE_FUN.1-3	ATE_COMP.1-1

NB: If the level of the assurance requirement chosen is higher than those identified in this table, the composite-specific work unit is also applicable.

[51] Machine Readable Travel Document with „ICAO Application", Basic Access Control.

ATE_COMP.1 Composite product functional testing

Objectives

The aim of this activity is to determine whether composite product as a whole exhibits the properties necessary to satisfy the functional requirements of its Security Target.

Application notes

A composite product can be tested separately and integrative. Separate testing means that the platform and the application are being tested independent of each other. A lot of tests of the platform may have been performed within the scope of its accomplished evaluation. The application may be tested on a simulator or an emulator, which represent a virtual machine.

Integration testing means that the composite product is being tested as it is: the application is running on the platform.

Behaviour of implementation of some SFRs can depend on properties of the underlying platform as well as of the application (e.g. correctness of the measures of the composite product to withstand a side channel attack or correctness of the implementation of tamper resistance against physical attacks). In such a case the SFR implementation shall be tested on the final composite product, but not on a simulator or an emulator.

This activity focuses exclusively on testing of the composite product as a whole and represents merely partial efforts within the general test approach being covered by the assurance ATE. These integration tests shall be specified and performed, whereby the approach of the standard assurance families of the class ATE shall be applied.

- A correct behaviour of the Platform-TSF being relevant for the Composite-ST (corresponding to the group RP_SFR-SERV and RP-SFR-MECH in the work unit ADV_COMP.1-1 above),and- absence of exploitable vulnerabilities (sufficient effectiveness) in the context of the Platform-ST are confirmed by the valid Platform Certificate, cf. chapter 6 above.

Dependencies:

No dependencies.

Developer action elements:

ATE_COMP.1.1D

The developer shall provide a set of tests as required by the assurance package chosen.

ATE_COMP.1.2D

The developer shall provide the composite TOE for testing.

Content and presentation of evidence elements:

ATE_COMP.1.1C

Content and presentation of the specification and documentation of the integration tests shall correspond to the standard requirements of the assurance families ATE_FUN and ATE_COV.

ATE_COMP.1.2C

The composite TOE provided shall be suitable for testing.

Evaluator action elements:

ATE_COMP.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Evaluator actions:

Action ATE_COMP.1.1E

ATE_COMP.1-1 The evaluator shall examine that the developer performed the integration tests for all SFRs having to be tested on the composite product as a whole.

In order to perform this work unit the evaluator shall analyse, for each SFR, whether it directly depends on security properties of the platform and of the application. Then the evaluator shall verify that the integration tests performed by the developer cover at least all such SFRs.

If the assurance package chosen does not contain the families ATE_FUN and ATE_COV (e.g. EAL1), this work unit is not applicable.

The result of this work unit shall be integrated to the result of ATE_COV.1−1C/ ATE_COV.1-1 and ATE_FUN.1.2C/ ATE_FUN.1-3 (or the equivalent higher components if a higher assurance level is selected).

Composite vulnerability assessment (AVA_COMP)

The composite-specific work units defined in this chapter are intended to be integrated as refinements to the evaluation activities of the AVA class listed in the following table. The other activities of AVA class do not require composite-specific work units.

CC assurance family	Evaluation activity	Evaluation work unit	Composite-specific work unit
AVA_VAN	AVA_VAN.1.3E AVA_VAN.1.3E AVA_VAN.1.3E AVA_VAN.1.3E	AVA_VAN.1-5 AVA_VAN.1-6 AVA_VAN.1-7 AVA_VAN.1-8	AVA_COMP.1-1 AVA_COMP.1-2 AVA_COMP.1-2 AVA_COMP.1-2

NB: If the level of the assurance requirement chosen is higher than those identified in this table, the composite-specific work unit is also applicable.

AVA_COMP.1 Composite product vulnerability assessment

Objectives

The aim of this activity is to determine the exploitability of flaws or weaknesses in the composite TOE as a whole in the intended environment.

Application notes

This activity focuses exclusively on vulnerability assessment of the composite product as a whole and represents merely partial efforts within the general approach being covered by the standard assurance family of the class AVA: AVA_VAN.

The results of the vulnerability assessment for the underlying platform represented in the ETR_COMP can be reused under the following conditions: they are up to date and all composite activities for correctness – ASE_COMP.1, ALC_COMP.1, ADV_COMP.1 and ATE_COMP.1 – are finalised with the verdict PASS.

Due to composing of the platform and the application a new quality arises, which can cause additional vulnerabilities of the platform which might be not mentioned in the ETR_COMP. In these circumstances [R44] applies.

Dependencies:

No dependencies.

Developer action elements:

AVA_COMP.1.1D

The developer shall provide the composite TOE for penetrating testing.

Content and presentation of evidence elements:

AVA_COMP.1.1C

The composite TOE provided shall be suitable for testing as a whole.

Evaluator action elements:

AVA_COMP.1.1E

The evaluator shall conduct penetration testing of the composite product as a whole building on evaluator's own vulnerability analysis, to ensure that the vulnerabilities being relevant for the Composite-ST are not exploitable.

Evaluator actions:

Action AVA_COMP.1.1E

AVA_COMP.1-1 The evaluator shall examine the results of the vulnerability assessment for the underlying platform to determine that they can be reused for the composite evaluation.

The results of the vulnerability assessment for the underlying platform are usually represented in the ETR_COMP. They can be reused if the following conditions are met: they are up to date and all composite activities for correctness – ASE_COMP.1, ALC_COMP.1, ADV_COMP.1 and ATE_COMP.1 – are finalised with the verdict PASS. The evaluator shall also consider the relevant determinations in the Platform Certification Report. For validity of the platform security certificate please refer to chapter 6 above. It is noted that the platform itself could be a composite TOE. This means also that the validity of each ETR for composition of the TOEs that compose the platform TOE must be checked.

When the validity of the ETRs for composition is checked, the necessity of checking the contents depends on the application and user available TSFI. If the TSFI are available to the user or used by the application, the content of the ETR must be checked. If not and formal platform TSFI are no longer available as TSFI, the validity date of the ETR_COMP is sufficient.

The result of this work unit shall be integrated to the result of AVA_VAN.1.3E/ AVA_VAN.1-5 (or the equivalent higher components if a higher assurance level is selected).

AVA_COMP.1-2 The evaluator shall specify, conduct and document penetration testing of the composite product as a whole, using the standard approach of the assurance family AVA_VAN.

If the correctness-related activities – ASE_COMP.1, ALC_COMP.1, ADV_COMP.1 and ATE_COMP.1 – are finalised with the verdict PASS and the certificate for the platform covers all security properties needed for the composite product, composing of the platform and the application must not create additional vulnerabilities of the platform.

If the evaluator determined that composing of the platform and the application creates additional vulnerabilities of the platform[52], a contradiction to the verdict PASS for the correctness activities has to be supposed or the certificate for the platform does not cover all security properties needed for the current composite product.

The result of this work unit shall be integrated to the result of AVA_VAN.1.3E/ AVA_VAN.1-6, AVA_VAN.1-7, AVA_VAN.1-8 (or the equivalent higher components if a higher assurance level is selected).

APPENDIX 2: ETR FOR COMPOSITE EVALUATION TEMPLATE

ENISA will develop an ETR for composition template that shall be used as a template by the Platform Developer to issue the ETR_COMP. https://www.sogis.eu/documents/cc/domains/sc/JIL-ETR-template-for-composition-v1-1.pdf is the current applicable template for the SOG-IS MRA related composite evaluations, which may serve as a technical basis for the EUCC scheme ETR for composition template.

APPENDIX 3: PLATFORM USER GUIDANCE EXAMPLES

Disclaimer: This section is not meant to be an appendix of an actual ETR for Composite evaluation but is included to support the platform developer in creation of user guidance requirements. These user guidance requirements have to be implemented by the embedded software developer in the application to protect the TOE against certain attacks.

User guidance requirements that are provided to the application developer must have the following properties:

1) It must be clear what the user has to do to protect the TOE
2) It must be clear for which attack (path or partial attack) the requirement is protecting from. The detail must be such that an embedded software developer will be able to perform a design compliance analysis. In other words, if a certain attack is not relevant for an application the formulation must be such that an application developer will recognise this.

[52] i.e. not mentioned in the ETR_COMP.

33. ANNEX 7: APPLICATION OF ATTACK POTENTIAL TO SMARTCARDS AND SIMILAR DEVICES

PURPOSE

This annex contains descriptions of attack methods that are specific for smartcards or similar devices and provides guidance metrics to calculate the attack potential required by an attacker to effect an attack. The underlying objective is to aid in expressing the total effort required to mount a successful attack. This should be applied to the operational behaviour of a smartcard or similar device and not to applications specific only to hardware or software.

PARTICULAR STATUS

None.

CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE

Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS.

1 INTRODUCTION

This Annex interprets the current version of the Common Criteria Methodology (CEM) (annex B.4) and provides guidance metrics to calculate the attack potential required by an attacker to effect an attack on a smartcard or similar device. The underlying objective is to aid in expressing the total effort required to mount a successful attack. This should be applied to the operational behaviour of a smartcard or similar device and not to applications specific only to hardware or software.

2 SCOPE

This document introduces the notion of an attack path comprised of one to many attack steps. Analysis and tests need to be carried out for each attack step on an attack path for a vulnerability to be realised. Where cryptography is involved, the Certification Body should be consulted.

3 FOREWORD: WORKLOAD FOR AVA_VAN.5 EVALUATION

No rigid rules can be given on how much time should be spent on a typical smartcard or similar device VAN.5 evaluation by a competent lab, but the following guidance shall nonetheless be provided in an effort to harmonise evaluations and the various national schemes alike: assuming the CC vulnerability analysis has already been performed the evaluation testing from scratch for a new IC should take about 3 man months, depending on the complexity of the IC such as the number of cryptographic services, interfaces, etc. The total evaluation time for composite evaluations using a certified IC for VAN.5 testing activities is of the order of 1-3 man months, depending on the complexity of the platform, such as open platform, native platform, number of APIs, etc.. It is possible to deviate from this guidance, but some reasoning will have to be provided to the Certification Body.

It is an assumption of this interpretation that the Certification Bodies will ensure that there is harmonisation not only nationally, but also between national schemes. This is required, for example, where new types of attack are applied and a decision has to be taken as to when the attack is considered ‘mature’, at which point it will no longer gain points for the time or expertise to develop the attack (as discussed below).

4 IDENTIFICATION OF FACTORS

In the Common Criteria there is no distinction between the identification phase and the exploitation phase of an attack. However, within the smartcard community, the risk management performed by the user of CC certificates clearly requires to have a distinction between the cost of “identification” (demonstration of the attack) and the cost of “exploitation” (e.g. once a script is published on the Internet). Therefore, this distinction must be made when calculating the attack potential for smartcard or similar device evaluations. Although the distinction between identification and exploitation is essential for the evaluation to understand and document the attack path, the final sum of attack potential is calculated by adding the points of these two phases, as both phases together constitute the complete attack.

4.1 How to compute an attack

Attack path identification as well as exploitation analysis and tests are mapped to relevant factors: elapsed time, expertise, knowledge of the TOE, access to the TOE, equipment needed to carry out an attack, as well as whether or not open samples or samples with known secrets had been used. Even if the attack consists of several steps, identification and exploitation need only be computed for the entire attack path.

The identification part of an attack corresponds to the effort required to create the attack, and to demonstrate that it can be successfully applied to the TOE (including setting up or building any necessary test equipment). The demonstration that the attack can be successfully applied needs to consider any difficulties in expanding a result shown in the laboratory to create a useful attack. For example, where an experiment reveals some bits or bytes of a confidential data item (such as a key or PIN), it is necessary to consider how the remainder of the data item would be obtained (in this example some bits might be measured directly by further experiments, while others might be found by a different technique such as an exhaustive search). It may not be necessary to carry out all of the experiments to identify the full attack, provided it is clear that the attack actually proves that access has been gained to a TOE asset, and that the complete attack could realistically be carried out. One of the outputs from Identification is assumed to be a script that gives a step-by-step description of how to carry out the attack – this script is assumed to be used in the exploitation part.

Sometimes the identification phase will involve the development of a new type of attack (possibly involving the creation of new equipment) which can subsequently be applied to other TOEs. In such a case the question arises as to how to treat the elapsed time and other parameters when the attack is reapplied. The interpretation taken in this annex is that the development time (and, if relevant, expertise) for identification will include the development time for the initial creation of the attack until a point in time determined by the relevant Certification Body and then harmonized under the EUCC scheme. Once this point in time has been determined, no additional points for the development of the attack (in terms of time or expertise) will be used in the attack potential calculation any more.

The exploitation part of an attack corresponds to achieving the attack on another instance of the TOE using the analysis and techniques defined in the identification part of an attack. It is assumed that a different attacker carries out the exploitation, but that the technique (and relevant background information) is available for the exploitation in the form of a script or a set of instructions defined during the identification of the attack. The script is assumed to identify the necessary equipment and, for example, mathematical techniques used in the analysis[53]. This means that the elapsed time, expertise and TOE knowledge ratings for exploitation will sometimes be lower for exploitation than for identification. For example, it is assumed that the script identifies such things as the timing and physical location required for a perturbation attack, and hence in the exploitation phase the attacker does not have to spend significant time to find the correct point at which to apply the perturbation. Furthermore, this same information may also reduce the exploitation requirement to one of mere time measurement, whereas the identification phase may have required reverse engineering of hardware or software information from power data – hence the expertise requirement may be reduced. Similarly, knowledge about the application that was used to achieve the timing of an attack may also be included either directly in the script or indirectly (through data on the timing required). As a general rule, no points can be awarded for the exploitation phase at all when, e.g., a secret master key common to all TOEs under investigation has been compromised in the identification phase. This is a consequence as the script defining details to be passed on between the identification and exploitation phase will already contain the information on this master key.

[53] This assumption is the worst-case scenario: The information obtained in a first attack (in the Identification phase) is fully shared with other attackers who wish to exploit this attack (Exploitation phase). This assumption is not always correct, in particular when the attack happens for commercial profit and sharing would have to happen between rivaling criminal organisations.

An example would be storing a master key in ROM and the ROM content has been read out, decrypted or descrambled during the identification phase.

In many cases, the evaluators will estimate the parameters for the exploitation phase, rather than carry out the full exploitation. The estimates and their rationale will be documented in the ETR.

To complete an attack potential calculation the points for identification and exploitation have to be added as both phases together constitute the complete attack. When presenting the attack potential calculation in the ETR, the evaluators will make an argument for the appropriateness of the parameter values used, and will therefore give the developer a chance to challenge the calculation before certification. The final attack potential result will therefore be based on discussions between the developer, the ITSEF and the CB, with the CB making the final decision if agreement cannot be reached.

4.2 Elapsed Time

Compared to the "Elapsed Time" factor as given in the CEM, further granularity is introduced for smartcards and similar devices. In particular, a distinction is drawn between one week and several weeks. The Elapsed Time is now divided into the following intervals:

Table 1: Rating for Elapsed Time

	Identification	Exploitation
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical (see below)	*	*

If an attack path has been identified and there are well-understood analysis results that allow to extrapolate the elapsed time for the actual security configuration of the TOE, then **Error! Reference source not found.** shall be extended by Table 1a:

Table 1a: Extra rating step for Elapsed Time

	Identification	Exploitation
> four months	6	10

It is not reasonable to expect an evaluation lab to spend extra time on the attacks. Hence, Table 1a only applies as a reasonable exception. And this exception must be justified with analysis/measurement results enabling to define a rationale for a scalable time factor in the attack. This means that e.g. intuition and success by chance are not sufficient criteria.

The CEM defines the term *Not Practical* as "the attack path is not exploitable within a timescale that would be useful to an attacker".

In practice an evaluator is unlikely to spend more than 3 months attacking the TOE. At the end of the evaluation the evaluator has to assess the time it would take to carry out the minimum attack path. This computes the estimated time to mount the attack, which is not necessarily the time spent by the evaluator to conduct the attack.

Extrapolation of results is intended to save cost and time, however if the rationale is solid but the developer challenges the results, extra testing needs to be performed. The Certification Body must be informed of such extra testing. Note that it shall be accounted separately from the workload initially scheduled and not replace other attacks.

Where the attack builds on the findings of a previous evaluation, Elapsed Time as well as Expertise have to be taken into account, e.g., a particular attack may have been developed on a smartcard or similar device with comparable characteristics to the TOE. It is not possible to give general guidance here.

The question of "Not Practical" may depend on the specific attack scenario as the following two examples show:

a) Consider a smartcard or similar device as TOE used for an online system, where the TOE contains only individual keys and assume further that these keys are deactivated in the system within days after loss of a card was reported. In this case an attack is not even practical if an attacker can extract the keys in one week.
b) Consider a smartcard or similar device as TOE, which contains system-wide keys, which might be used for fraud even if use of the individual card is blocked after loss. In this case an attack may be successful even if it takes a year.

So if a general assumption on a time for "Not Practical" is needed, something about 3-5 years is a better worst-case oriented time frame. (This is the time after which a card generation is normally exchanged and system wide keys may be changed in a comparable time frame). However, the best rule seems to be to decide on the meaning of "Not practical" only in a specific attack scenario.

4.3 Expertise

For the purpose of smartcards and similar devices, expertise levels are defined based on the attacker's ability to implement attacks, devise attack paths, develop attack setups and procedures, as well as the capability to understand the attack concepts, when applied to at least one out of the following domains (non-exhaustive list): HW manipulation, software attacks, cryptography, fault injection, side channel analysis, reverse engineering. Another factor defining the expertise level is attacker's capability to operate necessary tools and equipment (for a list of tool and equipment examples please refer to Table 9).

Table 2 contains detailed definitions and differentiating factors for the Expertise levels. In particular, the Expert attacker has the ability to not only understand complex concepts, but also to use this understanding in order to innovate and adapt. This includes creating new attack techniques, new attack paths, non-off-the-shelf setups or procedures, as well as, redesigning or adapting existing complex attack techniques, attack paths or procedures to apply them to the TOE. Innovation and adaptation capabilities are not expected from the Proficient attacker. The Proficient attacker's capabilities are limited to parameter adjustments such as the ones described in user manuals for benches and tools.

Table 2: Definition of Expertise

	Definition according to CEM	Detailed definition to be used in smartcard or similar device evaluations[54]
a) Experts	Familiar with - Implemented algorithms, protocols, hardware structures, security behaviour, principles and concepts of security employed, and - Techniques and tools for the definition of new attacks, cryptography, classical attacks for the product type, attack methods, etc.	• Having a capability to implement newly published attacks (typically based on a paper or a related patent), or a capability to devise new attack techniques or attack paths not addressable by off-the-shelf benches and tools and well prescribed and available sets of procedures. This also includes redesigning or implementing of attack techniques, attack paths, setups or procedures for well-established complex attacks, where the novelty or the need for adaptation is, for example, related to a specific target or implemented countermeasures. and • Having a deep knowledge or extensive training or experience in implemented algorithms, protocols, hardware structures, security behaviour, principles and concepts of security employed that allows for understanding the concepts of state-of-the art attacks and attack procedures. OR Having a capability to operate complex tools and equipment, that require expertise beyond what can be easily acquired from user's manual. This might, for example, include

[54] The logical operators in this column should be interpreted as: (clause 1 and clause 2) OR clause 3.

		expertise in material science or advanced imaging that is needed for intermediate result interpretation.
b) Proficient	Familiar with security behaviour of the product type	• Having a capability to perform attacks following previously developed and available procedures, where possible parameter adjustments have to be described in detail, such as the ones described in user manuals for benches and tools. and • Having basic knowledge, training, or experience in implemented algorithms, protocols, hardware structures, security behaviour, principles and concepts of security employed. OR Having enough practice and knowledge to operate off-the-shelf benches and tools, relying on available associated user's manuals.
c) Laymen	No particular expertise	No particular expertise

In case of ambiguities, the decisions about Expertise levelling should be made by ITSEF on a case by case basis. In particular, in certain cases such as for HW manipulation, if a set of procedures to perform the attack is well prescribed and available, but is very complex to execute, Expert attacker level can be considered. Conversely, if an exact set of non-complex procedures to perform a sophisticated attack is not prescribed and available, but only insignificantly differs from such available set, the attacker level can be considered as Proficient.

In addition, ITSEF should distinguish between the internal availability of developed attack procedures and their availability outside the ITSEF. This is important, especially in the case of consecutive evaluations of similar products. In particular, the rating should always reflect the difficulty of the entire attack path as if performed by non-ITSEF entities.

Both Proficient and Expert levels can be reached based purely on the ability to operate tools and equipment. An example of tools and equipment resulting in Expert rating are advanced Failure Analysis tools such as e.g. Focus Ion Beam station, which require extensive expertise to operate even when applied to attacks that are well established, well described and non-complex.

It may occur that for sophisticated attacks, several types of expertise are required. In such cases, the highest of the different expertise factors is chosen as mentioned in the CEM. In very specific cases, the "Multiple Expert" level could be used but it should be noted that the expertise must concern fields that are strictly different. For example experts, as defined in Table 2, in two or more out of the following domains (non-exhaustive list): HW manipulation, software attacks, cryptography, fault injection, side channel analysis, reverse engineering.

Table 3: Rating for Expertise

	Identification	Exploitation
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6

4.4 Knowledge of the TOE

Knowledge of the TOE refers only to classification levels related to the identification and exploitation of vulnerabilities in the TOE.

Care should be taken to distinguish information required to identify the vulnerability from the information required to exploit it, especially in the area of sensitive or critical information. It shall be clearly understood that any information required for identification shall not be considered as an additional factor for the exploitation. In general it is expected that all knowledge required in the Exploitation phase will be passed on from the Identification phase by way of suitable scripts describing the attack. To require sensitive or critical information for exploitation would be unusual.

The protection of the information will determine the classification of the information.

The knowledge of the TOE may graduate according to design abstraction, although this can only be done on a TOE by TOE basis. Some TOE designs may be public source (or heavily based on public source) and therefore even the design representation would be classified as public or at most restricted, while the implementation representation for other TOEs is very closely controlled and is therefore considered to be sensitive or even critical.

For the dissemination of information outside the developer organisation a distinction can be made between distributing information and providing access to information. Distributing information means handing over the information, thereby its use can not be (access) controlled anymore by the developer. Providing access means that the information will remain under the developer's control and its access will be controlled and protected. Different degrees can exist for distribution and access, as defined below.

The higher the classification, the more difficult it will be for an attacker to retrieve the information required for an attack. This specifically applies to all sensitive and critical information where a site audit is required to provide the necessary assurance on the sufficiency of security measures (See also CC ALC_DVS.2 if applicable).

Note that the developer organisation is defined as all organisations that are involved in the development and production phases of the product life-cycle that is subject of the evaluation (See also the CC ALC class). This means that e.g. a mask manufacturer subcontracted by the smart card developer is considered to be part of the developer organisation and its protection and access control measures are part of the evaluation.

Note: Since this annex defines the rating of attacks, the sharing of information during the evaluation with a trusted system of Certification Bodies and ITSEF(s) does not influence the classification below. A trusted system means that all Certification Bodies within this system trust each other.

Note: The ETR for composition (ETR_COMP) is a document controlled through the CC scheme which has issued the associated certificate. It is dedicated to be used by an ITSEF evaluating a composite product and does not enter in the rating of the attacks.

The following classification is to be used:

- **Public information** about the TOE (or no information): Information is considered public if it can be easily obtained by anyone (e.g., from the Internet) or if it is provided by the developer to any customer without further means.
- **Restricted information** concerning the TOE: Information is considered restricted if it is controlled within the developer organisation and distributed to other organisations under a non-disclosure agreement.
- **Sensitive information** about the TOE is knowledge that is only available to discrete teams[55] within the developer organisation. Sensitive information is protected by evaluated secure IT systems (e.g. through the requirements associated with Annex 2, MINIMUM SITE SECURITY REQUIREMENTS) and by appropriate environmental and organizational means. If such information needs to be distributed to or accessed by other organisations outside the developer, this must be limited to a strict need-to-know basis protected by a specific contract.
- **Critical information** about the TOE is knowledge that is only available to teams on strict need-to-know basis within the developer organisation. Critical information is physically and environmentally protected by high secure IT infrastructure as well as secure physical environment including attack detection and attack prevention layers. If such information needs to be accessed by other organisations than the developer, this must be limited to a strict need-to-know basis protected by a specific contract.
- **Very critical information** about the TOE is knowledge that is known by only a few individuals, access to which is very tightly controlled on a strict need to know basis and individual undertaking. The design of modern ICs involves not only huge databases but also sophisticated bespoke tools. Therefore, the access to useful data requires an enormous and time consuming effort which would make detection likely even with the support from an insider of the developer organization. If an attack is based on such knowledge the new level of "Very critical information" is introduced.
  Very critical information shall never be shared with organisations outside the developer without consulting the respective Certification Body that issues a certificate.
  It could occur that very critical information cannot be exported for technical reasons as the sophisticated

[55] All people involved in getting access to such information must be considered in the ALC activities.

bespoke tools of the developer are required to interpret the information or there is simply no interface for exportation or there is only a dedicated group of people – which can be different to the other groups of lower classification – specifically enabled to access this very critical information.
A review of such information is therefore usually only possible on the developer's premises. The common understanding of all parties of the evaluation should be that export of such information outside the developer's premises is an exceptional risk that should be avoided.

- Information is considered as *Not practical* if it is maintained by highly secured IT systems only (within sites protected as for very critical and critical information.

It may occur that for sophisticated attacks, several types of knowledge are required. In such cases, the highest of the different knowledge factors is chosen.

Table 4: Rating for Knowledge of TOE

	Identification	Exploitation
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical	9	*
Not practical	*	*

4.5 Access to the TOE

Access to the TOE is also an important factor. Generally, it rates the difficulty and effort to access and obtain samples of the TOE and is described in the following. In some cases, the TOE's package may create an additional barrier to access sensitive parts of the TOE. Therefore, the rating of 'Access to TOE' may be extended by considering the package as part of the TOE. The according methodology is described in Section 4.5.1.

It is assumed here that the samples of the TOE would be purchased or otherwise obtained by the attacker and that beside other factors there's no time limit in analyzing or modifying the TOE. The availability of samples (in terms of time and cost) needs to be taken into account as well as the number of samples needed to carry out an attack path (this shall replace the CEM factor "Window of Opportunity").

The attack scenario might require access to more than one sample of the TOE because:

- the attack succeeds only with some probability on a given device such that a number of devices need to be tried out,
- the attack succeeds only after having destroyed a number of devices (on average),
- the attacker needs to collect information from several copies of the TOE.

In this case, TOE access is taken into account using the following rating:

Table 5: Rating for Access to TOE

	Identification	Exploitation
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*

"Not Practical" is explained as follows:

- For identification: not practical starts with the lowest number between 2,000 samples and the largest integer less than or equal to n/(1+(log n)^2), n being the estimated number of products to be built.
- For exploitation: not practical starts with the lowest number between 500 samples and the largest integer less than or equal to n/(1+(log n)^3), n being the estimated number of products to be built.

As an example, if n equals 20,000 (samples produced), the "Not practical" limits would be 1,025 and 248 samples respectively for identification and exploitation.

The Security Policy as expressed in the Security Target should also be taken into account.

4.5.1 Rating the effort for TOE package preparation

For the cases where the vendor defined the package as part of the TOE, the package may consequently be part of an attack path and has to be considered for the identification and exploitation phase.

The following provides guidelines rather than absolute fixed values for the rating, as there is on one hand an uncounted variety of package types and materials and, on the other hand emerging methods and techniques which may not yet be publicly known for removal of those in the field.

Packages may occur, where a removal is difficult regarding methods and techniques and in such cases, the vendor has to support the evaluator with the required information. If there is still uncertainty, the evaluator should get in contact with external specialists, for example universities, institutes etc. in order to get a clear picture of how to rate the removal of such package.

The rating of attacks (e.g. fault injection, reverse engineering, side channel attacks, etc.) is rated independently from the package preparation effort. If the package is claimed to be part of the TOE a partial attack to prepare the package is rated by extra points for 'Access to TOE' as described in the following. This rating of the package preparation effort covers all other factors and therefore no further points shall be given elsewhere.

The guideline for the rating of the package removal considers the deviation into Low, Medium, and High preparation effort of the package. The definition of these terms and rating examples are given in Section A.1.

Table 6: Rating for TOE package removal (extra points in the factor 'Access to TOE')

	Identification	Exploitation
Low preparation effort	0	0
Medium preparation effort	1	2
High preparation effort	2	4

Low preparation effort: Simple packages that can be removed by standard chemical etching, mechanical action, re-wiring, or similar for the attack path.

Medium preparation effort: Packages that have a relatively high risk for fatal damage of the TOE (losing the functionality that is target or required for the evaluation) because of special constructions.

High preparation effort: Packages that require multiple experts, high effort and rare bespoke tooling which are not claimed as security functionality.

Note that if the reverse-engineering does not need to be redone in exploitation, consequently points in exploitation shall only be given if the remaining attack path still requires specialized equipment or above.

4.6 Equipment

Equipment refers to the hardware/software or cloud/online services that are required to identify or exploit the vulnerability.

In order to clarify the equipment category, price and availability have to be taken into account.

- **None**
- **Standard equipment** is equipment that is readily available to the attacker, either for the identification of vulnerability or for an attack. This equipment can be readily obtained e.g., at a nearby store or downloaded

from the Internet. The equipment might consist of simple attack scripts, personal computers, card readers, pattern generators, simple optical microscopes, power supplies, or simple mechanical tools.

- **Specialized equipment** is not readily available to the attacker, but could be acquired with increased effort. This could include purchase of moderate amounts of equipment (e.g., power analysis tools, use of hundreds of PCs linked across the Internet, protocol analyzers, oscilloscopes, microprobe workstation, chemical workbench, precise milling machines, etc.) or development of more extensive attack scripts or programs.
- **Bespoke equipment** is not readily available to the public as it might need to be specially produced (e.g., very sophisticated software) or because the equipment is so specialized that its distribution is controlled, possibly even restricted. Alternatively, the equipment may be very expensive (e.g., Focused Ion Beam, Scanning Electron Microscope, and Abrasive Laser Equipment). Depending on the possibilities of renting equipment and the type of manipulation to be performed, the classification of the equipment as bespoke might be reconsidered. Complex and dedicated software (e.g. advanced analysis tools that are not available for purchase) that has been developed during the identification phase can be considered as bespoke equipment or alternatively rated according to Elapsed time and Expertise criteria; it must not additionally be considered in the exploitation phase. If an evaluator has to adapt his dedicated analysis software, e.g. alignment tools/scripts or filters specifically to the TOE or TOE derivatives, then this has to be rated extra (Elapsed time, Expertise, Knowledge of the TOE, samples …) in the identification phase.
  Complex and dedicated software as introduced above can be characterised as being developed during the identification phase for the TOE under evaluation, or applied to another TOE while the ITSEF still considers it as beyond the state-of-the-art. In case there is uncertainty about the state-of-the-art, then discussion might be required at the relevant ECCG subgroup level.

It may occur that for sophisticated attacks several types of equipment are required. In such cases by default the highest of the different equipment factors is chosen.

Note, that using bespoke equipment should lead to a moderate potential as a minimum.

The level “Multiple Bespoke” is introduced to allow for a situation, where different types of bespoke equipment are required for distinct steps of an attack.

Table 3: Rating for Equipment

	Identification	Exploitation
None	0	0
Standard	1	2
Specialized [(1)]	3	4
Bespoke	5	6
Multiple Bespoke	7	8

[(1)] If clearly different test benches consisting of specialized equipment are required for distinct steps of an attack this shall be rated as bespoke. Test benches for side-channel and fault attacks are normally considered to be too similar and not different enough. In such cases where multiple similar specialized equipment is required, this will then be considered as Multiple Specialized and an additional 1 point will be added to the rating.

In an ideal world, definitions need to be given in order to know what are the rules and characteristics for attributing a category to an equipment or a set of equipment. In particular, the price, the availability of the equipment (publicly available, sales controlled by manufacturer with potentially several levels of control, may be hired) and the availability of operational resources involved shall be taken into account. Especially, the availability of operational resources involved has to be considered if bespoke equipment such as design verification or failure analysis tools has to be classified.

Manufacturers usually have information about the sophisticated tools market and where such equipment can be procured. Generally, manufacturers control the majority of the second hand tools market as well.

Efficient use of these tools requires either a very long experience or the human operator is hired together with the equipment. In other words, only a small number of dedicated, experienced experts operate the bespoke equipment. Nevertheless, one cannot exclude the fact that a certain type of equipment may be accessible through university laboratories or equivalent but still, expertise in using the equipment is quite difficult to obtain. Thus some consistency is expected between the ratings for expertise and equipment.

Please note, that in the case that additional operational resources are necessary this has also to be considered within the Expertise factor of the attack ranking table. The tables presented in the next section have been put together by a group of industry experts and will need to be revised from time to time as the range of equipment at the disposal of a potential attacker is constantly improving, typically:

- Computation power increase
- Cost of tools decrease
- Availability of tools can increase
- New tools can appear, due to new technology or due to new forms of attacks

4.6.1 Tools

The border between standard, specialized and bespoke cannot be clearly defined in all cases. As stated above, this decision shall be made on case by case basis depending on technology state-of-the-art, accessibility of tools, costs for purchasing and operational resources involved.

As a guide for evaluation, the equipment purchase price (whether it is new or refurbished) should be used as main distinguisher according to Table 8. The cost mentioned in this table is not the cost of an attack but only the purchasing market price of each equipment or workstation.

This distinguisher gives the best practical approach considering the equipment availability (respectively procurement). Additionally, it gives each category an assignment. This table will be regularly subject to updates following the equipment market evolution.

Table 8: Equipment rating versus purchasing cost

Purchasing cost	Equipment rating
Up to 10 K€	Standard
Between 10 K€ and 200 K€	Specialized
Over 200 K€	Bespoke

The following Table 9 provides typical examples using the chosen information of Table 8 and the general rules of the previous section and implements a general guideline.

Table 4: Categorisation of Tools

Tool	Equipment
Low-end light injection (UV, flash light)	Standard
Electrical glitches workstation	Standard
Binocular microscope	Standard
Thermal stress tools	Standard
Voltage supply	Standard
PC or workstation	Standard
Software tools (fuzzing, test suite)	Standard
Code static analysis tools	Standard
Low-end oscilloscope	Standard
High-end GPU card	Standard
Signal analysis tools	Standard
EMFI, FBBI workstations	Specialized
Optical microscope	Specialized
3D X-Rays workstation	Specialized

Micro-probing workstation	Specialized
High-end laser workstation	Specialized
Real time pattern recognition system	Specialized
High-end oscilloscope	Specialized
Spectrum analyser	Specialized
Wet chemistry tooling (acids & solvents)	Specialized
Dry chemistry (Plasma)	Specialized
Micro-milling and thinning machine	Specialized
Low-end Scanning Electron microscope (SEM)	Specialized
EM signal acquisition workstation	Specialized
Low-end Emission Microscope (EMMI)	Specialized
Low-end Focus Ion Beam (FIB)	Specialized
High-end Scanning Electron Microscope (SEM)	Bespoke
Atomic Force Microscope (AFM)	Bespoke
High-end Focused Ion Beam (FIB)	Bespoke
New Tech Design Verification and Failure Analysis Tools	Bespoke
High-end Emission Microscope (EMMI)	Bespoke
Chip reverse engineering workstation	Bespoke

4.7 Open Samples/Samples with known Secrets

In certain cases, it is opportune to use special samples within the evaluation process. In the following these samples will be called “open samples” or “samples with known secrets”. The use of the “open samples” or “samples with known secrets”, its scope, and the implications on the evaluation and the attack rating are described in this section.

4.7.1 Clarification of the notions of platform, application and HW-TOE

In a composite evaluation as a rule, the properties of the underlying platform are taken from the information supplied with the documentation from the certification of the underlying platform. Annex 6, COMPOSITE PRODUCT EVALUATION FOR SMART CARDS AND SIMILAR DEVICES specifies the process, called “composite smart card evaluation”. In that annex, platform and application are relative notions and generic terms. A platform can be, for example, a certified IC with its firmware, a certified Embedded Software, or a combination of both. The certified platform is used as the basis for the composite evaluation. An application is the additional Embedded Software that is added on top of the certified platform. It can be, for example, an Operating System on a certified IC, an application on certified IC and Operating System such as an application on a Java Card product or a combination of Operating System and applications on certified IC. The notions of platform and application that are used in the sections below correspond to those used in Annex 6.

In many cases, the fundament for all subsequent certifications of smart cards and similar devices is the hardware IC certificate. This hardware IC certificate includes at least the HW-IC and firmware to operate it but can include also additional software providing for example cryptographic services to the user. The combination of IC hardware, firmware and additional software comes with dedicated user guidance documents also belonging to the corresponding TOE definition.

Additional software components in a HW IC evaluation use the notion of “application” on top of the HW IC and Firmware. The definition of open samples in the sense of the composite evaluation of applications given in the next chapter, also applies to additional SW components, that are evaluated in the context of a HW IC certification.

For the combination of the HW IC and the firmware, HW-TOE is used as a shortcut in the following sections.

4.7.2 Definition of “open samples / Samples with known Secrets”

Within the context of a HW-TOE evaluation, excluding SW components, the term “open sample” stands for samples with the capability to download and/or run any kind of test software. In addition such samples may allow insecure configurations of the HW-TOE, e.g. to bypass countermeasures of the firmware or to change the internal configuration of the IC hardware. This might include support of specific testing enviroments by the vendor as an operating system package is not included in the HW-TOE. The IC hardware shall not be changed as it would raise validity questions and it is as well not justifiable in terms of cost that the vendor changes the IC hardware just for the purpose of the evaluation.

Within the context of a composite evaluation, or for SW components in the HW-IC certification, the term “open samples” stands for samples where the evaluator can put applications on the platform or the HW-TOE at his own discretion that bypasses countermeasures prescribed in the platform guidance or countermeasures implemented in the applications themselves. The intention is to use test applications without countermeasures but not to deactivate any countermeasures inherent to the platform, or the HW-TOE respectively.

For a composite evaluation, the test application may serve to highlight platform properties described in the ETR_COMP considering the special use of the platform in the TOE but may not be used to repeat the platform evaluation.

In addition, another possibility is to enable the evaluator to define one or more pieces of secret data for an asset of the TOE, such as a PIN or key, where this ability would not be available under the normal operation of the TOE. These samples will be named as “Samples with known secrets” and can be used to perform attacks on this asset without deactivating countermeasures. To enable the evaluator to define secret data for one asset does not mean that this information shall be used to attack another asset of the TOE.

If the normal TOE configuration gives the opportunity to the ITSEF to have full control of input and output data, the use of the term “samples with known secrets” cannot be applied. However, “samples with known secrets” can be considered even during HW evaluation if the vendor gives specific access to internal secrets. For example: cryptographic mechanisms used internally by the HW-TOE, such as used for memory encryption.

Please note, that every functional interface or key necessary for the functional tests of the TOE provided by the vendor to the ITSEF shall not be considered as an “open sample / sample with known secrets”.

4.7.3 Use of “open samples / Samples with known Secrets”

In some special cases the vulnerability analysis and definition of attacks might result in an attack path that is difficult or in the worst case impossible to be evaluated because it would need considerable time or would require extensive pre-testing, if only knowledge of the TOE is considered.

Additionally, the platform may be used in a way that was not foreseen by the platform developer and the platform evaluator, or the application developer may not have followed the recommendations provided with the platform and implemented different countermeasures where the effectiveness is not yet proven.

Finally, the composite evaluator has to consider parts of the platform functionality that may not have been covered by the Security Target of the platform and therefore the previous platform evaluation.

Different possibilities exist to shorten the evaluation time in such cases:

- The composite evaluator can consult the evaluator of the underlying platform and draw on his experience gained during the evaluation with the consent of the platform vendor.
- Separation of countermeasures within the application and countermeasures of application and platform with the use of “open samples”.
- Accelerate the evaluation especially where cryptographic operations are involved by using “samples with known secrets”. With these samples the evaluator knows the “secret” (key). This allows either comparison of retrieved data (e.g. as deduced from passive analysis) against the “known secret”. “Open samples” may be useful in a profiling step required for some attacks such as template attacks. The evaluator therefore has a simplified way to determine if his attack has revealed the correct secret. He can stop after retrieving parts of the “secret” and estimate the remaining time to find the complete “secret”.

In order to keep an efficient and meaningful evaluation in a maintainable time as mentioned before, it can be necessary to use “open samples / samples with known secrets”. In such case, certain rules should be followed:

- The purpose of open samples / samples with known secrets is to set up tests for the evaluation and not, in the case of a composite evaluation, to repeat the platform evaluation.
- The use of open samples / samples with known secrets, the information flow between parties and if necessary the support of extra services is discussed and agreed upon between the Certification Body, the

evaluator, the developer and the developer of the open samples. This also includes the time spent for tests with the open samples / samples with known secrets.

- Failures and observations resulting from the tests are communicated and made known at least to the Certification Body of the TOE. In case of a composite evaluation, the Certification Body of the composite TOE shall take appropriate steps together with the Certification Body of the underlying platform evaluation in accordance with rules of Annex 6.
- The rating shall make provision for the judgement whether or not the attack would have been possible without the use of “open samples / samples with known secrets” (see section 4.7.5).

4.7.4 Implications on evaluations

With the use of “open samples / samples with known secrets”, it is possible to enable or to factorise attack paths and by that reduce the complexity of an attack. That saves time in the evaluation because it makes it possible to obtain the targeted result much faster.

Open samples may allow to perform a leakage assessment prior to any side-channel attack by evaluating the leakage with and without additional countermeasures. Thereafter, the TOE can be validated with an appropriate attack method.

If leakage was found by switching off additional countermeasures and if a theoretical assessment could be done, the number of traces necessary to successfully attack the TOE can be estimated. To get comparable results in evaluations where no leakage assessment is done, the time frame or number of traces of the acquisition campaign has to be limited beforehand and the theoretical estimation has to be compared against this limit.

Another good example for open samples is the retrieving of secret information (e.g. keys) by light attacks. In a well-designed product, the platform as well as the application will have protective mechanisms to avert this attack. In combination, they will make attacks quite difficult. The evaluator will have to try a very high number of combinations and variations of parameters like beam diameter, light frequency, light energy, location for applying the light, position in time for the light flash. This gets especially difficult if the application contains means to render the TOE inoperable if an attack is detected. An attack could not only prove very time consuming but also require a great number of samples.

With “open samples”, the situation is quite different. The evaluator can use his own optimised test program and scan the IC for “weak spots” much faster and without risking the destruction of the device. He can also optimise his efficiency at a found “weak spot” before switching back to attack the TOE. Even if one would know about the existence of “weak spots”, still the optimization and the choice of the best spot has then to be done on the final TOE. With the use of “open samples” in these tests the attacker can then launch much more directed attacks on the TOE.

The following examples describe the usage of “samples with known secrets”, for instance:

- To extract the complete key might prove to be very time consuming. With some errors in the retrieved key and no possibility to decide which part of the secret is incorrect, an attack might not be possible due to timing constraints.
- A profiling stage is sometimes required to perform some attacks, such as template attacks. Knowing the key, and then the intermediate values of the algorithms, may then make an attack possible whereas the attack would have been not practical without the use of such samples.

4.7.5 Calculating the attack potential

An additional factor is defined in the attack potential table for “open samples / samples with known secrets” with points given in the identification phase only. Due to the definition of “open samples / samples with known secrets” it is clear that these are forbidden to be used in the exploitation phase.

When rating an attack that makes use of “open samples / samples with known secrets”, the evaluator must first fairly determine (at least theoretically) and describe the way in which an attacker could carry out the attack on the real TOE (instead of on the open sample/sample with known secrets). Having determined this, the evaluator will perform two calculations with and without using “open samples / samples with known secrets”:

- Estimating the value for each factor for an attacker without access to open samples / samples with known secrets.
- Giving the values for each factor corresponding to what he has done (had he completed the entire attack):
  - Time spent, destroyed samples, Expertise, Knowledge of the TOE, Equipment
  - Adding the points corresponding to the “open samples / samples with known secrets” used.

Should it turn out that:

1) the attack is “Not practical” when not using open samples or samples with known secrets, and

2) the rating of the “open sample/sample with known secrets” factor in the field is not public, and

3) the developer formally asserts that the function used on the open sample is not an accessible feature available for users on a device on the field,

then the rating is “Not practical” (i.e. the “open samples / samples with known secrets” rating must be discarded). If the developer changes his formal assessment, a reassessment of the TOE has to be done.

In all other cases the final value will be the minimum of the two calculations. It is expected that the two values are quite close. If this is not the case, further analysis is required to decide on the rating.

Where “open samples / samples with known secrets” exist, collusion (or direct attack, such as theft) to obtain them is possible in the same way that the evaluation takes into account a possible collusion or direct attack for an attacker to get information as defined in the chapter about knowledge of TOE.

For “samples with known secrets”, defining the protection level is part of the evaluation of the full product.

The points corresponding to the availability of “samples with known secrets” are defined by taking into account the level of access control to the secret provided by the sample and the protection of the secret inside and outside the developer’s organization during the entire life cycle:

- Public:

  The secret is accessible without any restrictions (public documents, sample allowing to know the secret,…).

- Restricted:

  The secret is controlled within the developer’s organization. Outside the developer’s organization all people who have signed the NDA could have access to the secret.

  If the secret can be released by the sample it must be protected by access control with credentials, which are protected as restricted secrets.

- Sensitive:

  Inside or outside the developer’s organization, secrets are only shared by discrete teams or devices clearly identified, with strong access controls. Handling of the secret is governed by specific and appropriate written procedures to protect it, and there is a clear method by which the secret is identified as requiring these procedures (e.g. by labelling the data).

  If the secret has to be distributed to other organisations, this must be on a strict need-to-know basis protected by a specific contract. The other organisation must provide a secure environment which is evaluated or compliant by contract with criteria acceptable by the Certification Body.

  If the secret can be released by the sample, it must be protected by access control with credentials, which are protected as sensitive secrets.

- Critical:

  The Secret is not shared outside the developer’s organization.

  Inside the developer’s organization, secrets are only shared by few people or few devices clearly identified, with strong access controls on a need-to-know basis. Handling of the secret is governed by specific and appropriate written procedures to protect it, and there is a clear method by which the secret is identified as requiring these procedures (e.g. by labelling the data). It could be applied to the following examples:

  - HW Key split between mask and Flash or PUF or other.
  - Signing keys for firmware update in the field.

  If the secret can be released by the sample it must be protected by access control with credentials, which are protected as ‘Critical’ secrets.

- Not practical:

  The secret is not shared outside the developer's organization.

  The developer has no possibility to know the secret. The sample can not release the secret. For example:

  - Keys completely generated inside the device.
  - Keys generated inside an HSM, not accessible by the developer, and transferred to the TOE through secure channel in a secure environment

Table 5: Rating for Samples with known secrets

	Identification	Exploitation
Public/Not required	0	NA
Restricted	2	NA
Sensitive	5	NA
Critical	9	NA
Not practical	*	NA

The points corresponding to the availability of "open samples" are defined by taking into account the number, the protection and control of these open samples during the entire life cycle:

- Public:

  Open samples: No protection of the samples, delivered without control (no NDA, no checking of the customer).

- Restricted:

  Open samples are protected and controlled within the developer's organisation and can be distributed to other organisations under an NDA.

- Sensitive:

  Open samples must be limited in number, protected and controlled within the developer's organisation. If the samples have to be distributed to other organisations, this must also be limited in number and to a strict need-to-have basis protected by a specific contract. The other organisation must provide a secure environment which is evaluated or compliant by contract with criteria acceptable by the Certification Body.

- Critical:

  Critical open samples are never to be distributed outside the developer's organisation. Within the developer's organisation they must be limited in number and are only available to teams on a strict need-to-have basis. Critical open samples are physically and environmentally protected by a secure evaluated physical environment.

The usage of an "open sample" is more powerful than having access to a "sample with known secrets" as it might allow to get access to secrets that are ranked 'Not practical' for the TOE.

Table 11: Rating for Open Samples

	Identification	Exploitation
Public/Not required	0	NA
Restricted	2	NA
Sensitive	5	NA
Critical	9	NA

Please note that sharing of “open samples / samples with known secrets” for the evaluation purpose with a trusted system of Certification Bodies and recognized ITSEF(s) does not influence the classification above.

In specific cases where the “open samples / samples with known secrets” categorization matches an intermediate classification level, the final rating granted for such samples would need to be addressed with the concerned CB(s) on a case by case basis.

The ITSEF has to define if the use of “open samples” and “samples with known secrets” accumulates the efforts in time during the evaluation and add points for each of them.

For platforms, the protection level of “open samples / samples with known secrets” will be analysed during the underlying platform evaluation and stated in the ETR_COMP.

The wording “Sibling Product” refers to products available in the field that have interesting features in common with the TOE, with less countermeasures activated and/or more functions available. Those products may not have implemented as many countermeasures as the TOE or may have more functions because their security problem is different from the TOE's. When the ITSEF uses a feature from an Open Sample delivered for the evaluation, the Developer provides an analysis addressing the threat of “Sibling Products” also offering this feature. In case the threat remains applicable, the rating related to the protection of the open sample (presented in the list above) has to be adapted by also considering the availability of a “Sibling Product”. In cases where the availability of the “Sibling Product” would be ranked as public but it is not public knowledge that the “Sibling Product” can be used as a substitute of the used open sample then a rating of ‘Restricted’ is applied instead to cover the effort of identifying the “Sibling Product” and of using it as a substitute to the open sample.

4.7.6 Good usage of open samples and guidance for correct rating

As the privileged usage of open samples / samples with known secrets can be very efficient to speed up evaluations, it also introduces pitfalls that must be avoided. The examples below provide some advice and good practices to correctly require and use open samples / samples with known secrets.

General remarks

As mentioned previously, the goal of the factor open sample / sample with known secrets is to allow an efficient and meaningful evaluation in a maintainable time. The ITSEF must provide a motivated request to the developer explaining the purpose of the open samples / samples with known secrets with respect to the practical tests that will be done on the TOE. This includes a description of the attack path without using open samples / samples with known secrets as well as the estimations of the two different rankings. If an agreement between the CBs, the ITSEF and the developer is achieved, the developer will ask the developer of the open sample to provide the open samples / samples with known secrets to the ITSEF. Asking for open samples / samples with known secrets systematically without having in mind the setup of a potential attack derived from the vulnerability analysis is not considered a good practice and shall be declined.

ITSEF should also clearly distinguish between the advantages of using the open sample during an ongoing evaluation from the transferable advantages obtained during other evaluations. If the transferable advantages were gained using open samples from other evaluations, then the rating of this sample also has to be transferred and shall be used in the attack ranking. This is important, especially in the case of evaluations of similar products.

Synchronization on specific operations of interest

Vulnerability analysis requires precise synchronization. This is usually much easier to achieve with an open sample that allows the execution of dedicated code. The open sample could provide some specific trigger signals to indicate e.g. the start and/or end of the operation of interest.

In case of a HW-TOE evaluation firmware modification, or other changes of internal configurations, deviating from the normal product configuration may allow additional synchronization features. Here, the open sample could also be a sample where certain power-saving features (e.g. dynamic Voltage-Frequency scaling), that make some test runs unusable due to unpredictable timing behavior, or performance enhancements (e.g. CPU caches) have been deactivated.

Activation of an available internal interface

Some TOEs have a special interface that may reveal internal data for validation purposes. If this interface is already available and accessible without HW modification, the developer could authorize the ITSEF to use such data in the vulnerability analysis. For example, this could be a sample that exposes the TRNG interface for entropy testing. Here, the interface, which is normally used for validation, and also necessary for TRNG entropy assessment, is used to observe loss of entropy more directly than usually possible. This kind of sample is then rated as open sample.

Pitfalls on attack rankings with and without open samples
Consider here the example of fault attacks where the evaluator has the possibility to find weak spots thanks to open samples, the rating of the attack with and without open samples must be calculated.

Without open samples, the attack on the TOE (combination of platform + application) might not be realistic and might be unfeasible as the number of TOEs needed during the identification phase might reach the 'Not practical' ranking. It is really important to carefully evaluate and not to minimize the influence of the usage of open samples on each factor. Otherwise the usage of open samples would lead to an unjustified rating and in the extreme to a fail of the product if the ranking without open sample is not correctly and fairly done.

Procedure to rank supervised learning attacks using open samples
In case of profiled or supervised learning attacks such as template attacks, supervised machine learning or supervised deep learning approaches it is necessary to possess a sample where the secret information, that is intended to be learnt, can be set to arbitrary values or is known. If this can only be achieved using an open sample the procedure described at the beginning of section 4.7.5 has to be followed. Especially paragraph 88 has to be taken into account as these kinds of attacks are not practical if the learning phase of the attack cannot be applied.

Additionally, there exists the threat that the learning phase could be conducted on a different product and used to attack the TOE. Therefore, the wording of a "Sibling Product" and a procedure that was introduced above has to be followed to address this threat.

Considerations on loading test applications in 'Open platform' evaluations
During 'Open platform' evaluations, loading test applets can help the ITSEF to validate quickly, deeply or with more accuracy the robustness of some specific features. For that purpose, loading capabilities are given to the ITSEF. The points attributed for this advantage need to be considered when the full attack path is rated.

Please note that the knowledge of one loading key of an 'Open platform' will not allow to load applets on all products based on the same platform. Usually more than one set of loading keys exists and may be distributed to different vendors.

For the full attack path rating, either the loading mechanism is broken – and effort to break the loader must be rated in the full attack path – or one of the loading key sets must have been compromised to the attacker. In that case 'open samples / samples with known secrets' points shall be given.

The number of points will be rated according to 'open samples / samples with known secrets' definitions and depends on the protection effort of the loading keys of the platform under evaluation that must be defined by some additional rules provided in the Security Target or in a related security document such as guidance. For example, if no statement is provided about the loading keys management in the ST or in product guidance the ITSEF will consider the minimum criteria factor (Public). If the developer is selling exactly the same platform on different products with different levels of loading keys protections the same rules as for samples with known secrets must be applied.

Obviously, if the loading keys are used by the ITSEF to allow the loading of an applet only providing functional interfaces towards services and that does not provide any significant advantage for the attack realization (no change in factor categories inducing a rating change, e.g. interval change for Elapsed time) no points will be given.

4.8 Calculation of attack potential

Table 12 identifies the factors discussed in the previous sections and associates numeric values with the two aspects of identifying and exploiting a vulnerability. It replaces Table B.3 of CEM for products that fall under the technical domain of "Smart Cards and similar devices".

Table 12: Final table for the rating factors

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
> four months[56]	6	10
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical	9	*
Not practical	*	*
Access to the TOE (1)		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (2)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples / Samples with known secrets		
Public/Not required	0	NA
Restricted	2	NA
Sensitive	5	NA
Critical	9	NA
Not practical (Samples with known secrets only)	*	NA

(1) If the package has been claimed as being part or contributing to the TOE security, then extra points to the category 'Access to TOE' may be given as described in Section 4.5.1and in Table 6.

[56] See Section 4.2 for applicability of this factor.

[2] If clearly different testbenches consisting of specialised equipment are required for distinct steps of an attack this shall be rated as bespoke. Testbenches for side-channel and fault attacks are normally considered to be too similar and not different enough. In such cases where multiple similar specialized equipment is required, this will then be considered as Multiple Specialized and an additional 1 point will be added to the rating.

* Indicates that the attack path is not exploitable in a manner that would be useful to an attacker. Any value of * indicates a High rating.

The following table replaces Table B.4 of the CEM and should be used to obtain a rating for the vulnerability.

Table 13: Rating of vulnerabilites and TOE resistance

Range of values*	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

*final attack potential = identification + exploitation.

5 EXAMPLES OF ATTACK METHODS

The following examples have been compiled by a group of security experts representing the different actor groups involved in the development, production, security evaluation and distribution of a smartcard product (hardware vendors, card vendors, OS provider, evaluation labs, Certification Bodies, service providers).

The collection represents the current state of the art at the time. As state of the art is not static this document is under review and will be updated if necessary.

For the evaluation of a TOE at least these examples have to be considered. This does not mean that in any case all attacks have to be carried out, nor should this catalogue of attacks be considered as an exhaustive list. On the contrary, the manufacturers and labs are encouraged to search for new attacks and attack variants as part of their evaluation activities. For each TOE the evaluation lab conducting the evaluation will select the appropriate attacks from this catalogue in agreement with the Certification Body. This selection will be dependent on the type of the TOE and additional tests are likely also required.

In this document only a general outline of the attacks is given. For more detailed descriptions and examples, please refer to the Certification Bodies. They can also provide examples as reference for rating.

5.1 Physical Attacks

5.1.1 General description

Microelectronic tools enable to either access or modify an IC by removing or adding material (etching, FIB, etc). Depending on the tool and on its use the interesting effect for the attacker is to extract internal signals or manipulate connections inside the IC by adding or to cutting wires inside the silicon.

Memories could also be physically accessed for, depending on the memory technology, reading or setting bit values.

5.1.2 Impact on TOE

The attack is directed against the IC and often independent of the embedded software (i.e. it could be applied to any embedded software and is independent of software counter measures).

The main impacts are:

- Access to secret data such as cryptographic keys (by extracting internal signals)
- Disconnecting IC security features to make another attack easier (DPA, perturbation)
- Forcing internal signals
- Even unknown signals could be used to perform some attacks

The potential use of these techniques is manifold and has to be carefully considered in the context of each evaluation.

5.2 Overcoming sensors and filters

5.2.1 General description

This attack covers ways of deactivating or avoiding the different types of sensor that an IC may use to monitor the environmental conditions and to protect itself from conditions that would threaten correct operation of the TOE. Hardware or software may use the outputs from sensors to take action to protect the TOE.

Sensors and filters may be overcome by:

- Disconnection
- Changing the behaviour of the sensor
- Finding gaps in the coverage of the monitored condition (e.g. voltage), or of the timing of monitoring.

Sensors may also be misused, in order to exploit activation of a sensor as a step in an attack. This misuse of sensors is a separate attack.

The different types of sensors and filters include:

- Voltage (e.g. high voltage or voltage spike)
- Frequency (e.g. high frequency or frequency spike)
- Temperature
- Light (or other radiation)

5.2.2 Impact on TOE

Under this attack, the correct operation of a chip can no longer be guaranteed outside the safe operating conditions. The impact of operating under these conditions may be of many sorts. For example:

- Contents of memory or registers may be corrupted
- Program flow may be changed
- Failures in operations may occur (e.g. CPU, coprocessors, RNG)
- Change of operating mode and/or parameters (e.g. from user to supervisor mode)
- Change in other operating characteristics (e.g. changed leakage behaviour; enable other attacks like RAM freezing, electron beam scanning).

If a chip returns incorrect cryptographic results then this may allow a DFA attack, see section **Error! Reference source not found.**. Other consequences are described under general perturbation effects in section **Error! Reference source not found.**.

5.3 Perturbation Attacks

5.3.1 General description

Perturbation attacks change the normal behaviour of an IC in order to create an exploitable error in the operation of a TOE. The behaviour is typically changed either by operating the IC outside its intended operating environment (usually characterised in terms of temperature, Vcc and the externally supplied clock frequency) or by applying one or more external sources of energy during the operation of the IC. These energy sources can be applied at different times and/or places on the IC.

The attacks aim at protecting mechanisms and typically include the following:

- Reducing the strength of cryptographic operations,
- Tampering with memory protection mechanisms,
- Affecting non-volatile monotonic counter values.

Creating faults can be used to recover keys or plaintext, to change the results of validation such as authentication or lifecycle state checks, to change the program flow, to provide unauthorized access to protected memory or to enable rollback and replay attacks.

Section **Error! Reference source not found.** concerns itself more with the methods to induce meaningful faults whereas section **Error! Reference source not found.** describes how these induced faults may be used to extract keys from cryptographic operations.

5.3.2 Impact on TOE

Perturbations may be applied to either a hardware TOE (an IC) or a software/composite TOE (an OS or application running on an IC).

For attackers, the typical external effects on an IC running a software application are as follows:

- Modifying a value read from memory during the read operation: The value held in memory is not modified, but the value that arrives at the destination (e.g. CPU or coprocessor) is modified. This may concern data or address information.
- Modifying a value that is stored in volatile memory. The modified value is effective until it is overwritten by a new value, and could therefore be used to influence the processing results or the security policy of the device.
- Modifying non-volatile monotonic counter values used to ensure the data freshness. Glitching or reducing the voltage of the power supply at the counter increment can result in a marginal value giving a possibility to roll the counter back, thus enabling replay attacks (if no special countermeasures, like a checksum of a counter, are implemented).
- Changing the characteristics of random numbers generated (e.g. forcing RNG output to be all 1's) – see Section **Error! Reference source not found.** "Attacks on RNG" for more discussion of attacks on random number generators.
- Modifying the program flow: the program flow is modified and various effects can be observed:
  - Skipping an instruction
  - Replacing an instruction with another (benign) one
  - Inverting a test
  - Generating a jump
  - Generating calculation errors

It is noted that it is relatively easy to cause communication errors, in which the final data returned by the IC is modified. However, these types of errors are not generally useful to an attacker, since they indicate only the same type of errors as may naturally occur in a communication medium: They have not affected the behaviour of the IC while it was carrying out a security-sensitive operation (e.g. a cryptographic calculation or access control decision).

The range of possible perturbation techniques is large, and typically subject to a variety of parameters for each technique. This large range and the further complications involved in combining perturbations means that perturbation usually proceeds by investigating what types of perturbation cause any observable effect, and then refining this technique both in terms of the parameters of the perturbation (e.g. small changes in power, location or timing) and in terms of what parts of software are attacked. For example, if perturbations can be found to change the value of single bits in a register, then this may be particularly useful if software in a TOE uses single-bit flags for security decisions. The application context (i.e. how the TOE is used in its intended operating environment) may determine whether the perturbation effect needs to be precise and certain, or whether a less certain modification (e.g. one modification in 10 or 100 attempts) can still be used to attack the TOE.

5.4 Retrieving keys with FA

5.4.1 General description

By using Fault Analysis (FA), an attacker intends to obtain information about a secret key by analysing the difference between a correct and a faulty cryptographic output, or by analysing different faulty cryptographic outputs.

This attack method requires analysing faulty outputs. Such faulty output could be obtained by inducing a physical perturbation on the device during the corresponding cryptographic computation, or eventually during the algorithm parameters manipulation. Such perturbation can be created by either non-invasive (power glitching for instance) or semi invasive (laser typically) techniques.

According to the theory behind this attack, the fault injected during the device processing should fulfil specific requirements to lead to an exploitable output. For most attacks, these requirements are based on both a precise synchronisation and the expected value as a consequence of the perturbation. A lack of accuracy in these requirements can render the analysis to recover the key much more complex.

From a practical point of view, the process to mount such an attack can then be divided into the following stages:

- Searching for a suitable fault injection method

- Depending on the cryptographic algorithm to attack, setting up a more or less accurate synchronisation technique.
- Inducing fault(s) during the device's execution and then collecting the corresponding faulty cipher texts
- Analysing the differences between the faulty cipher texts with the correct cipher text (or eventually the plain text).

5.4.2 Impact on TOE

This attack can be carried out in a non-invasive or an invasive manner. The non-invasive method (power glitching) avoids physical damages. The invasive method requires the attacker to physically prepare the TOE to facilitate the application of light on parts of the TOE.

DFA can break cryptographic key systems, allowing to retrieve DES, 3DES and RSA keys for example, by running the device under unusual physical circumstances. The attacker needs to inject an error at the right time and location to exploit erroneous cryptographic outputs.

As keys and code are usually present in EEPROM it might be difficult to randomly alter bits without crashing the entire system instead of obtaining the desired faulty results, although code alteration can give results as well. Other techniques may be useful to determine best location and time to inject an error; such as analysing the power consumption to determine when the cryptographic computation occurs.

5.5 Side-channel Attacks – Non-invasive retrieving of secret data

5.5.1 General description

Side-channel attacks target secret information leaked through unintentional channels in a concrete, i.e. physical, implementation of an algorithm. These channels are linked to physical effects such as timing characteristics, power consumption, or electromagnetic radiation.

SPA and DPA stand for 'Simple' and 'Differential Power Analysis', respectively, and aim at exploiting the information leaked through characteristic variations in the power consumption of electronic components, usually without damaging the TOE. Although various levels of sophistication exist, the power consumption of a device can in essence be simply measured using a digital sampling oscilloscope and a resistor placed in series with the device.

When an IC is operating, each individual element will emit electromagnetic radiation in the same way as any other conductor with an electrical current flowing through it. Thus, as this current varies with the data being processed, so does the electromagnetic radiation emitted by the TOE. Electromagnetic Analysis (EMA) attacks target this variant of information leakage. These attacks are sometimes referred to as SEMA (Simple Electromagnetic Analysis), or DEMA (Differential Electromagnetic Analysis). They may use emissions from the whole IC (chip-EMA), or may focus on the emissions from particular areas of the die, where critical components are located (local-EMA).

Experimental evidence shows that electromagnetic data (particularly from localised areas of a die) can be rather different from power trace data, and ICs that are protected against power analysis may therefore be vulnerable to EMA.

For the sake of unity in what follows SPA and DPA will denote not only attacks based on measurements of the power consumption, but are understood to cover their "cousins" in electromagnetic attacks as well, unless stated otherwise.

Implementations that include countermeasures like Boolean masking that resist first order DPA may be vulnerable to higher-order DPA. This attack requires that the attacker is able to correlate more than one data point per TOE computation using hypotheses on intermediate states that depend on secret key parts.

The combined statistical analysis for higher-order DPA may be based on aligned measurements of the same side channel at different times or on aligned simultaneous measurements of different channels such as power consumption and electromagnetic radiation of the device during the computation.

The outcome of a side-channel attack may be as simple as finding a characteristic trigger point for launching other attacks (such as DFA), or as complete as the secret key used in a cryptographic operation. It can also aim at recovering other secret data such as PINs, or random numbers generated for use as secrets, or even the opcode of the code being executed on the TOE. Depending on the goal of the attack it may involve a wide range of methods from direct interpretation of the recorded signal to a complex analysis of the signal with statistical methods. In the latter case the initial filtering used for signal analysis will generally depend on the type of the measurement (i.e., power consumption or electromagnetic radiation), but the mathematics for retrieving the secret information eventually is largely the same.

5.5.2 Impact on TOE

It lies in the very nature of SPA and (higher-order) DPA attacks that they may in principle be applied to any cryptographic algorithm – either stand-alone, e.g., for retrieving secret keys or PINs, or as part of a composite attack. Additionally, SPA may serve as a stepping stone for launching further attacks. For instance, SPA may be employed to detect a critical write operation to the EEPROM that needs to be intercepted. An SPA analysis may also be performed as part of a timing attack (e.g., in the square-and-multiply algorithm of RSA), or for deducing which branch of a conditional jump has been taken by the program flow. Or it could simply be used as a first step for identifying countermeasures to side-channel attacks that need to be overcome. Finally, an SPA attack could be employed to determine the proper trigger point for a subsequent glitch or light attack, or as an aid for localising a suitable time window for a physical probing attack

A DPA (or template) attack does not need to be entirely successful for it to become dangerous. Given a suitable key search strategy that takes into account imperfect DPA results as discussed further below, it may be enough to retrieve only part of the secret key by DPA, and obtain the rest by brute-force methods.

Implementations that resist DPA attacks may still be vulnerable to higher-order DPA attacks since that type of attack is tapping additional information not considered in a standard attack. Of course, algorithms that are vulnerable to first-order DPA are vulnerable to higher-order DPA, too. It appears that higher-order DPA is particularly suited to deal with Boolean and arithmetic masking / blinding of symmetric algorithms. On the other hand, the extension of higher-order DPA to public key (asymmetric) algorithms seems to be very difficult, because of the widely applied blinding countermeasures that make use of algebraic transformations during the calculation that are completely different from ordinary masking.

Power analysis as well as EMA attacks may be carried out for a hardware TOE (an IC), or a software/composite TOE (an OS or application running on an IC). Some countermeasures may already exist in the hardware TOE, whilst others are added later in software. Thus, the way in which software uses the IC functions may make a critical difference to its vulnerability to this type of attack.

5.6 Exploitation of Test features

5.6.1 General description

The attack path aims to enter the IC test mode to provide a basis for further attacks.

These further attacks might lead for example to disclosure or corruption of memory content, a change in the lifecycle state, or deactivation of security features. But as this depends on the possibilities of the test mode, the details about those further attacks are not considered here.

5.6.2 Impact on TOE

As result of successful access to the IC test mode, the attacker might be able to:

- Read out the content of the non-volatile memory using test functions. The implementation of the test functions may have an impact on the usability of the retrieved user data.
- Re-configure the life cycle data or error counters using a test function. Thereby an attacker is able to continue his analysis on the same device, even when a lifecycle status change would otherwise have stopped him.

5.7 Attacks on RNG

5.7.1 General description

Attacks on RNGs aim in general to get the ability to predict the output of the RNG (e.g. of reducing the output entropy) which can comprise:

- past values of the RNG output (with respect to the given and possibly known current values),
- future values of the RNG output (with respect to the possibly known past and current values),
- forcing the output to a specific behaviour, which leads to:
    - known values (therefore also allowing for the prediction of the output),

- unknown, but fixed values (reducing the entropy to 0 at the limit),
- repetition of unknown values either for different runs of one RNG or for runs of two or more RNGs (cloning) .

A RNG considered here can be one of the following types[57]:

- true RNGs (TRNG), the output of which is generated by any kind of sampling inherently random physical processes,
- pseudo RNG (PRNG) which output is generated by any kind of algorithmic processing (the algorithm is in general state based, with the initial state (seed) may generated by a TRNG),
- hybrid RNG (HRNG), which consists of a TRNG and a PRNG with a variety of state update schemes.

The applicable attack methods vary according to the Type of RNG.

A true RNG may be attacked by[58]:

- permanent or transient influence of the operating conditions (e.g. voltage, frequency, temperature, light)
- non invasive exploitation of signal leakage (e.g. signal on external electrical interfaces)
- physical manipulation of the circuitry (stop the operation, force the line level, modify and/or clone the behaviour, disconnect entropy source)
- wire tapping internal signals (compromise internal states)

A pseudo RNG may be attacked by:

- direct (cryptographic) attack on the deterministic state transition and output function (e.g. based on known previous outputs of the RNG)
- indirect attack on the state transition computation process by employing some side channel information (i.e. leakage on external electrical interfaces)
- attack on the execution path of the processing (modification of the results)
- attack on the seed (prevent reseeding, force the seed to fixed known or unknown (but reproducible) value, compromise the seed value)
- exceed the limit of RNG output volume (e.g. forcing the RNG to repeat values or to produce enough output to enable the attacker to solve equations and based on the solution to predict the output)

The attacks on hybrid RNG will be in general a combination of attacks on TRNGs and PRNGs.

All RNG designs can be expected to demand also for test procedures to counter attacks like those listed above. The analysis above does not take attacks on test procedures into account, as such attacks will by covered sufficiently by the more general attack scenario on software. Observe that test procedures may be an object on attack like SPA/DFA to reveal the RNG output values.

5.7.2 Impact on TOE

A successful attack on the RNG will result in breaching the security mechanisms of the chip, which rely on the randomness of the RNG. The mechanisms may be DPA/SPA countermeasures, sensor testing, integrity checking of active shield, bus and/or memory encryption and scrambling. The application software is affected by such attacks indirectly, e.g. if sensors and related tests being disabled by an attacker then this will generate further attack possibilities.

The software developer can rely on the capabilities of the hardware platform for testing the RNG and use these or implement and perform additional tests by himself based on such capabilities. The software developer may implement also tests for repetition of RNG output, but the coverage and feasibility of such tests may depend on the implementation and seems to be a problem. The cloning attack for RNG output on different instances of a RNG cannot be countered by tests, so other mechanisms must be designed as appropriate.

In case of TRNGs, sufficient tests should be performed (either by the chip platform itself or by the software developer). AIS31[59] is an example of a methodology for assessing the effectiveness of the testing mechanisms. In the case of PRNG, special effort on protecting the seed and the algorithm in terms of integrity and confidentiality is

[57] In the context of smart cards the RNG based on some measurements of environment are not considered to be relevant.
[58] It is here assumed that the direct attack on a true RNG (i.e. guessing the value) is not feasible for any attacker.
[59] Functionality classes and evaluation methodology for physical random number generator, Version 3, 15.05.2013 (BSI).

required. This effort relates to general software and data protection aspects and will not be discussed further in this section.

5.8 Ill-formed Java Card applications

5.8.1 General description

This logical attack consists in executing ill-formed applications, i.e. malicious applications that are made of illegal sequences of byte-code instructions or that do not have valid byte-code parameters.

This example is only applicable to Java Cards (although there may be equivalent attacks for other operating systems). If not combined with any other attack such as authentication bypass, this attack has to be applied to Java Cards with known loading keys (these could be considered as open samples). In addition, if the card includes an embedded byte-code verifier, this verifier must be disabled. No other specific configuration is required.

Ill-formed applications execute a sequence of byte-code that violates the Java rules. Ill-formed applications are usually created from standard applications, in which the byte-code is manually modified. It means that such ill-formed applications cannot be the output of a normal CAP file generator. As a consequence, most Java Card platforms do not enforce the rules during the execution of applications.

5.8.2 Impact on TOE

In the most successful cases, the attacker can retrieve information (e.g. a dump of memory), execute functions that usually require specific privileges or even switch to a context giving full control over the card (JCRE context).

5.9 Software Attacks

Most of the examples of attacks in this document require hardware attack steps for all or part of the attack. However, it is clear that there are many relevant attacks that can be made on software alone. This section considers some of these attacks. In many cases software attacks start with source code analysis or extensive software testing. Both are usually combined for more efficiency on the coverage of vulnerabilities detection.

In general, it is important to note that most software attacks arise from:

- errors (bugs) in the TOE, either in design or implementation;
- inconsistency, holes or ambiguity in the specification or standards;
- exploitation of sensitive or critical knowledge obtained on the TOE.

In the case of errors (bugs), it will generally result in a failure to meet the requirements of one (or more) of the ADV families. Hence an error of this sort will cause the TOE to fail evaluation (or, more usually, will require a modification to the TOE to correct the error).

In the case of issues coming from the specification or standards, the modification of the design’s specification may be insufficient to meet the TOE security objectives: for example, a protocol specification might itself contain critical vulnerabilities. This would also cause a TOE to fail the evaluation.

In the case of exploitation of knowledge of the TOE, the attacker may have access to authentication data for example, opening the usage of some features only accessible for the developers. For example, the attacker may use proprietary administration commands requiring authentication.

This section therefore lists a number of attack steps that may be used to discover software errors. If any error is discovered then it must be corrected if the TOE is to pass evaluation.

In the text below we consider first an information gathering attack step, which may be relevant to a number of different types of attack. We introduce five specific attack techniques that may exploit software vulnerabilities:

- Information gathering on commands
- Direct protocol attacks
- Man-in-the-middle and replay attacks
- Buffer overflow or stack overflow
- Communication interface switching

Attacks related to application isolation (loading, firewalls, etc.) are not described in this section but in section **Error! Reference source not found.** “**Error! Reference source not found.**”

The attacks are of a logical nature, to perform such attacks, it is necessary to have:

- a means to listen to message sequences (reader, traffic analyser)
- a means to create messages (information on external API, pattern generator)
- a means to interrupt messages without detection (protocol dependent)
- a means to analyse the source code with a tool
- a means to create applications
- a means to build and run larger test suites

So the test environment may consist of:

- A PC
- a smart card reader
- test software for test scripts writing and execution and communicating with the smart card
- a source code analysis tool (for white box testing or memory dump analysis)
- a protocol analyser (for reverse engineering of communication protocols)
- a development environment (for development of applications to load on the TOE)

Setting up a test environment and identifying an attack could be done in rather short time, as the following applies:

- the tools are considered to be standard equipment (some software tools are even available as freeware on the Internet),
- the commands are often ISO standard and therefore public knowledge,

However:

- tools usage and interfacing with the equipment for building the test scripts may require some significant set-up time,
- if the command set is proprietary, the expertise needed is slightly higher because the communication must be interpreted.

Note that if the security level is based on ‘security by obscurity’, it would not be considered a valid defence against attack.

The expertise of the attacker could be proficient or expert, and may be multiple expert, especially when combining very precise areas of expertise (Java Card and cryptography for example).

5.9.1 General description

This type of attack aims to get unauthorised access to data residing on the smartcard to perform operations which do not match the current lifecycle state of processed data objects or of the Operating System. As an example, such an attack aims to read or modify personalised data that resides on the card or aims to perform a further (unauthorised) initialisation or personalisation of the product.

Getting unauthorised access to data stored on the smartcard can be obtained by various techniques:

- Impersonating the other side of the communication (known as ‘man-in-the-middle’),
- using timing differences (by capturing and replaying commands),
- trying command variations (either editing valid commands or finding undefined commands),
- manipulation of access rules themselves,
- circumvention or manipulation of the request and evaluation of access rules during program execution.

Executing commands that are not allowed in the current lifecycle state of the Operating System or of a data object can also be obtained by various techniques:

- manipulation of the current lifecycle state itself,
- circumvention or manipulation of the request and
- evaluation of the current lifecycle state during program execution, and
- trying command variations (either editing valid commands or finding undefined commands).

The manipulations of lifecycle state information and access rules require a logical attack on the smartcard and its Operating System and applications. The circumvention and manipulation of the request and evaluation of lifecycle state information and access rules is based on a manipulation of the intended program flow that may be achieved by logical means (physical means are not considered in this example).

In the rest of this section, different type of software attacks techniques are described and have to be considered as elementary building bricks: usually, a full attack path is a combination of the different techniques.

5.9.2 Information gathering on commands

5.9.2.1 Overview

By their nature, communication protocols are susceptible to information leakage. This unwanted effect is a consequence of the fact that they are designed to pass information. This type of attack tries to use the protocols in ways that were not intended by the protocol developer, by first gathering information and then changing that communication to obtain secret data or other resources.

The attack step is usually a non-invasive technique, with the aim of getting information on the communication commands that the smartcard supports or using information from message sequences to enable other attacks. It is noted that the information is assumed to be information not contained in design documents (e.g. undocumented responses to commands). This information may then enable the attacker to modify the interaction or to disclose information (e.g. user data or keys) using weaknesses in the software implementation. This attack step is normally not a full attack path leading to the retrieval of secret data, although it might do in specific cases (exposure of secret data in this way would generally be considered a sufficient vulnerability to cause the TOE to fail evaluation[60]).

This attack step results in gathering information on the operation of the TOE. The information gathered is analysed to see whether it can be used to mount an attack to retrieve secret data from the TOE with one of the other mechanisms described in this document. The attacker knows the attack has succeeded by analysing the answers the smartcard gives during the communication.

5.9.2.2 Attack Step Descriptions

Observing Message Sequences

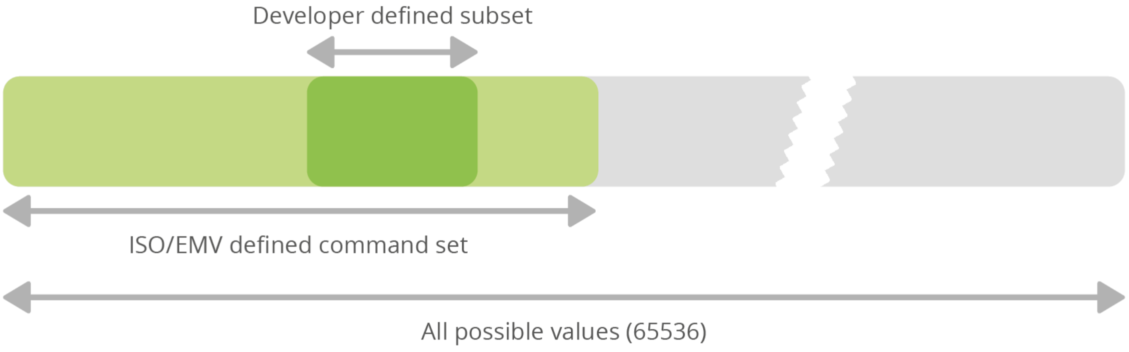
Observing message sequences may result in:

- obtaining information on an unknown protocol (e.g. where the interface specification is not public) to prepare an attack
- obtaining information on unknown internal product structures (typically data structures in software) to prepare an attack
- disclosing information, keys, or security attributes during import or export operations
- tracing product activity or user behaviour (e.g. to enable a replay attack).

Such observation is only possible when intercepting a valid communication between a smart card and a terminal. If the attacker does not have such possibility, he has to proceed with the next step "Command searches".

Command searches

The total amount of values that a smartcard can communicate using a typical protocol such as ISO 7816 T=1 is 2^{16}, or 65536 different commands. Of this set, ISO defined a subset as being valid commands. And of this ISO set, a developer defines a subset and documents these commands as being valid commands for this card.



[60] Depending on the scope of the evaluation and the environment, there may be some situations where such information exposure is accepted, e.g. in a protocol for use only in secure personalisation environments.

A T=1 test plan may contain the following tests:

- A ‘brute force’ approach in which all values outside the ISO defined set are tried and it is checked whether the card responds (inopportune behaviour).
- A ‘brute force’ approach in which all values of the ISO defined set, but outside the developer defined set are tried for a response (undocumented command search).
- Trying all developer documented commands and checking the answers.
- Trying all developer documented commands, but with emphasis on limit cases and multiple error cases.
- Influencing the communication by sending commands in different sequences.
- Interrupting message from system or from product

Attacks that make use of undocumented commands and editing commands are closely related, but distinctive attacks. Finding undocumented or undefined commands is a straightforward brute-force type of attack, where the attacker simply runs the ISO defined set of commands to see if the card replies to one or more commands that it should not answer to.

However, if source code is not available, simple command search of valid CLA/INS pair is not sufficient, as especially in the context of identification of existing commands: sometimes all CLA/INS/P1/P2/Lc have to be correct. So it represents 2^{40} or 1 099 511 627 776 different possibilities (see ISO/IEC 7816-4 standard).

Though an undocumented command search can be highly standardized and automated, the identification could be brief or very costly in terms of time, or even too costly to be considered as practical. Once all variations of parameters are tried and the answers are recorded, the attacker analyses if there is any interesting attack mount point. Once an interesting answer has been determined the attacker builds a script to discover the behaviour of the identified command and exploit a potential vulnerability. This could also be done by source code checking. Note that finding a single command may not be sufficient, as the attacker may have to look for a specific sequence of commands, sometimes following a proprietary protocol.

Whether the undocumented command may present attack points depends on the quality of the software (the separation of execution domains) and the type of command that is discovered.

Editing commands

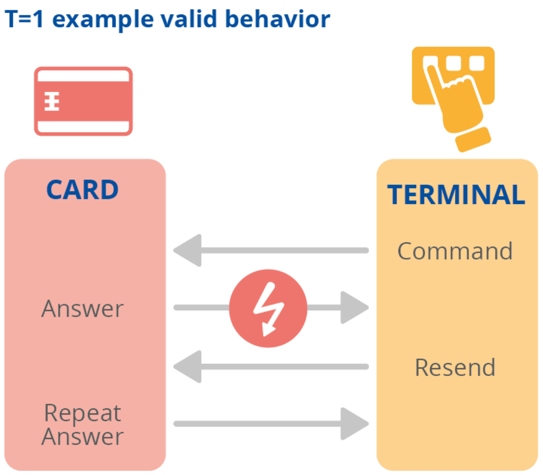
Editing commands is an attack step where the attacker tries to modify commands during the communication sequence to see if the card gives an unexpected reply (these commands may be in an interface specification, or they may have been discovered by observing message sequences or a command search as described above). These attack steps may enable vulnerabilities to be discovered and exploited (e.g. editing previously observed messages to supply a parameter that is too long may enable a buffer overflow attack). They may also expose timing differences that assist in reverse engineering of the software.

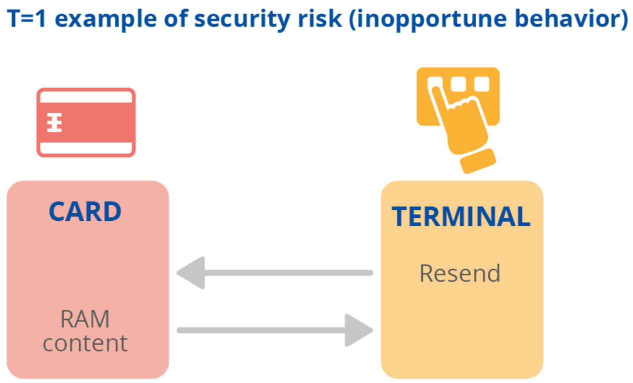
According to the security mechanisms associated to the API and the type of message, it may be easy or complex to forge a message (Mutual authentication, Secure channel, MAC, Ciphering, session key,...). However, as noted earlier, if an attack of this sort can be found then it will generally cause a TOE to fail evaluation.

5.9.3 Direct protocol attacks

A typical protocol attack is to try to send commands that the smartcard does not expect in its current state. For example: the ISO 7186-3 and 14443 protocols for smartcards contain a command for handling failure in the communication. Instead of starting a genuine communication, by sending this command an attacker may receive an un-initialized buffer, or the last buffer that was written.

This example is shown in the following pictures.





In this example, whether the TOE actually dumps the memory contents depends on the proper initialisation of I/O buffer pointer and length. The memory shown in the example might contain residual secret data, for example a recently calculated DES session key. Therefore this attack may allow an attacker to retrieve secret data from the TOE.

Under the category direct protocol attacks, there are also attacks focusing on the state machine of the TOE, where some sensitive operations need a specific order. Such order may ensure that the keys used in the cryptographic calculations are not exposed (such as challenge sending before a signature).

5.9.4 Man-in-the-middle and Replay attacks

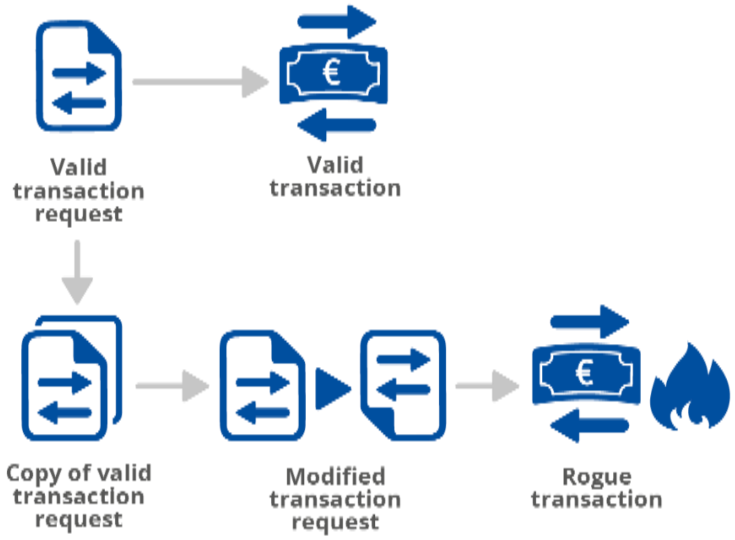
In this attack, the attacker hides in the communication path between two entities that are executing a valid communication. The attacker presents himself to either party as the other (valid) party. Some applications of man-in-the-middle attacks in public literature may be found in the following papers:

- An Example of a Man-in-the-middle Attack Against Server Authenticated SSL-sessions, Mattias Eriksson
- Man-in-the-Middle in Tunnelled Authentication Protocols, N. Asokan, Valtteri Niemi, Kaisa Nyberg, Nokia Research Center, Finland
- Why Cryptosystems Fail, Ross Anderson

Man in the middle attacks are based on valid command interception either to perform replay attacks or to change some of the parameters to compromise the exchange of data (get access to confidential data exchanged, modify the parameters exchanged).

Replay attacks are possible when a mechanism does not check that a command is a genuine part of the current message sequence, or that a complete message sequence has not been used before (in general, a secure protocol should prevent this sort of attack by design[61]). An attacker uses a protocol analyser to monitor and copy packets as they flow between smartcard and reader or host. The packets are captured, filtered and analysed for interesting information like digital signatures and authentication codes. Once these packets have been extracted, the packets are sent again (replayed), thus giving the attacker the possibility to get unauthorized access to resources.

[61] Even where a protocol is designed to be secure, it may be possible to use a replay attack if a further attack step (such as a perturbation) is used to avoid a check that would otherwise detect and reject the replayed commands.


Valid transaction request
Valid transaction
Copy of valid transaction request
Modified transaction request
Rogue transaction

The picture shows a situation where the attacker copies a valid transaction request, modifies it and sends a second request using the same (or slightly modified) versions of the messages. In general this type of attack might allow the attacker to get unauthorised access to a user's assets, for example a bank withdrawal or access to protected system resources.

The attack may be a full attack path, such as if a bank account withdrawal succeeds. In the case where system resources are accessed, it might be a partial attack path, depending on the nature of the resources that are accessed (e.g. as a result of the attack the attacker may be able to communicate as an ordinary user and may then try to gain privileged status).

The replay attack might be countered by using sequence numbers with appropriate integrity protection, making the use of recorded valid messages much harder.

5.9.5 Buffer overflow or stack overflow

This attack is applicable to any embedded software or firmware. An example is given below for an open platform. Open platforms are defined in this document as smart card operating systems with the capability of running and downloading multiple applications.

Open platforms provide a set of services to applications, in particular services to protect their sensitive data against external applications (unauthorized access and unexpected modification).

This attack could be performed through buffer overflow or stack overflow, produced by the execution of a malicious application. Overflow, when not checked by the platform, can have various effects, such as overwriting existing content in the current stack.

The expected effect by the attacker here is that the malicious application modifies the current execution context and obtains system privileges. For example, the execution rights of the current context is written in the stack; if the attacker can overwrite these rights and put the administrator rights, all operations performed after this operation will have the administrator rights. As another example, the attacker may overwrite a memory location that contains a pointer in memory. The attacker may then control where an application is getting its data.

Gaining such privileges allows this application to execute virtually every operation and then disclose or modify secret data, e.g. modifying or disclosing the PIN of another application.

Another effect is that internal data or data that were not presumed to be returned by a command are retrieved.

5.9.6 Communication interface switching

This attack is applicable to dual interface cards. The purpose is to exploit the possibility to communicate with a TOE on two different interfaces.

For example, on a TOE inserted in a mobile phone with a NFC interface, the TOE can be accessed either by the NFC interface or by the applications downloaded in the phone (communication in contact mode). The attacker may wait for a valid mutual authentication between the terminal and the TOE, and then through the contact interface, the attacker could communicate with the TOE to take advantage that a secure session is opened. This is a way for the attacker to bypass a state machine chaining and to get access to commands with a privileged access.

5.10 Application isolation

5.10.1 Introduction

A multi-application platform describes a set of hardware and software built with the aim to run more than one application at the same time.

The combination of the physical and logical measures of the multi-application platform allows the application isolation, which might be defined as: all the security measures and mechanisms which protect the sensitive assets from the application and the platform against modification and/or disclosure.

The assets that may need to be protected in a multi-application environment are:

- Loaded application data (including keys).
- Loaded application code.
- Underlying platform data.

Applet isolation is the target of various types of attack techniques to reach these assets. As such, the multi-application platform is subject to the typical Smart Card attacks, such as:

- Physical attacks,
- Perturbation attacks,
- Side Channel attacks and,
- Software attacks, which may or may not be combined with the above-mentioned attacks, detailed as:
    - Unauthorized disclosure of Loaded Application data (such as application data, code and keys).
    - Unauthorized use of instructions, commands or sequence of commands.
    - Bypassing the Administrator restrictions by loading a malicious application on the multi-application platform.
    - Read confidential data or code belonging to another Loaded-Application without authorization by using a Loaded-Application.
    - Modify data or code belonging to another Loaded-Application without its authorization, by using a Loaded-Application.
    - Access the confidential data of system resources (like a system patch), by using the Loaded-Application.
    - Reverse-engineer the abstraction layer mechanisms by Using the Loaded-Application

5.10.2 Partial attacks

There is an existing set of technologies applicable to ensure the isolation of applications. These technologies are usually specified in standards, and can be combined in smart card devices.

When performing a full attack, an attacker may need to defeat one or a combination of these technologies. The term partial attacks is used here to describe attacks that have to be combined in the performance of a full attack.

5.10.3 GlobalPlatform partial attacks

The GlobalPlatform (GP) standard comes with the definition of a framework for application interoperability and management. This framework is specified by the GP specification and we can identify the main components as follows:

- Open GlobalPlatform Environment (OPEN)

OPEN is an additional layer to the JCRE which provides extra management functionalities to the card. If present on the card, the OPEN is responsible for command dispatching, (optional) multiple logical channel management, management of application and card lifecycle.

The OPEN provides also a concrete management for performing the installation and deletion of applications. For this, the GP specification defines the notion of a security domain.

- Security domain (SD)

A security domain represents a smart card actor on the card. Three main actors may be present on the card: an application provider (AP), a card issuer (CI) and a controlling authority (CA). SD is a special kind of a smart card application which provides common security services for applications which are associated to it e.g. various kinds of cryptographic services, secure messaging as well as application personalization. A SD stores cryptographic secrets of the actor which it represents. A GP card is always provided with a CI security domain. One of the benefits which SDs bring to security providers is that an AP may benefit of a certain independence with respect to the CI mainly for provisioning of security services (e.g. secure messaging, or application personalization) to its associated applications. A SD may be granted further privileges which would enable it to perform Card Content Management (application load, installation etc.).

- Cardholder verification methods

These are the common security services which the card provides to all applications. In particular, this gives the possibility for a unique user PIN number to be used by all applications.

5.10.3.1 Description of a partial attacks

The aim of attacking GlobalPlatform is to allow an attacker to illegally load an application onto the TOE, *i.e.*, without knowing the loading keys values.

The attack is not performed on the cryptographic computations involved in the GlobalPlatform mutual authentication process and subsequent secure messaging commands.

The attack is performed on the code execution of the security domain with content management privilege. The attack exploits here a potential vulnerability in the robustness of the code execution flow against perturbation attacks. The idea is here to force the execution of any content management APDU command (INSTALL [for load], LOAD, etc) whereas no secure channel has been opened. If the implementation is basic, this may consist in a simple verification such as:

```
if (securityLevel == SecureChannel.NO_SECURITY_LEVEL)
ISOException.throwIt(0x6985);
```

Then, the attacker simply needs to send a content management command (without previous INITIALIZE UPDATE and EXTERNAL AUTHENTICATE command) and if it specifies a 0x80 CLA byte, no secure channel unwrapping will be processed: therefore no cryptographic computations have to be attacked.

For a successful applet loading and installation, two distinct sequences are required:

- A sequence for code loading, consisting in an INSTALL [for load] and one or several LOAD commands;
- A sequence for applet instantiation, consisting in an INSTALL [for install & make selectable] command.

In the first sequence, the attacker shall be able to reproduce the attack successfully on all the commands within the sequence as the loading operation is atomic (at least 2[62]). If the attack fails (which generally implies a power off), the sequence shall restart from the initial INSTALL [for load] command.

5.10.3.2 Impact on TOE

The direct impact is that the TOE may contain malicious code that could disclose or alter other applications.

5.10.4 Bytecode verifier partial attacks

All bytecodes must be verified before their execution in order to avoid the execution of malformed applets. In the Java technology, the ByteCode Verifier is used to verify the class file on the Java Virtual Machine and is operating dynamically (ex: applied each time a class is loaded). However, the full ByteCode Verifier is often not implemented in a Java Card due to its limitation in processing power and memory size. There are several solutions to resolve this issue:

- The application can be verified off-card by an Off-Card Verifier which is not limited by Java Card constraints.
- The application can be verified on-card with a specific On-Card Verifier designed for Java Card.

[62] An optimized malicous applet that is able to execute code loaded into the heap (*e.g.*, in arrays content) can fit in a single LOAD APDU command. Otherwise, an average of about 2 or 3 LOAD commands is to be considered.

The Java Card Protection Profile specifies that all bytecode should be verified before its execution. Additional verifications to ensure that the application does not contain malicious code are also required. If all verifications succeed, the CAP file can be loaded onto the card.

In this context, the TOE is the smart card because all the assets to protect are in it. There is no asset in the Off-Card Verifier. In fact, this attack allows an attacker to ask for loading its malicious applet without being detected.

5.10.4.1 Description of a partial attack example

Basic type confusion attacks modify the reference of an object by the reference of another object. For instance, we can assign the address of a byte array to a short array in order to dump memory located after the byte array. The two following attacks are based on type confusing:

- Create a type confusion not detected by an On-Card Verifier enabling us to dump and modify a part of the memory content.

Several steps are necessary for this attack. First, it is needed to characterise the On-Card Verifier in order to understand its behaviour and to analyse checks performed by this tool. Secondly, it is needed to write the malicious applet by creating a type confusion not detected by the On-Card Verifier.

The main assumption of this attack is that the application could be loaded on card. If it is not the case, this attack will become a combined attack. In fact, the evaluator should use an attack described in section **Error! Reference source not found.** “**Error! Reference source not found.**” in order to bypass the loading mechanism.

- Using a well-formed CAP file abusing the transaction mechanism in order to create a type confusion.

The aim of this attack is to create a type confusion using a weakness in the implementation of the platform enabling us to dump and modify a part of the memory content. This type of attack uses a well-formed CAP file and abuses the transaction mechanism in order to create a type confusion.

The main assumption of this attack is that the application could be loaded on card. If it is not the case, this attack will become a combined attack. In fact, the evaluator should use an attack described in section 5.10.3 “GlobalPlatform partial attacks” in order to bypass the loading mechanism.

5.10.4.2 Impact on TOE

The impact of the type confusion attack is dependent of software implementation.

The main impacts are:

- Retrieve secret data (such as cryptographic keys).
- Read data/code outside our context.
- Modify data of another application.
- Modify the source code of another application.

5.10.5 Defensive virtual machine partial attacks

There are two approaches in maintaining type safety within virtual machines

- Semi-defensive virtual machine: all bytecodes are either verified before or during installation (off-card or on-card)

The semi-defensive virtual machine prevents type confusion by disallowing certain bytecode execution sequences. Both virtual machines with off-card and on-card bytecode verifiers are considered semi-defensive virtual machines.

- Defensive virtual machine: type safety is enforced at run-time because the virtual machine only references typed data

The defensive virtual machine[63] can analyze the bytecode dynamically during the APDU execution (ex: type verification and structural verification) and does not require off- or on-card bytecode analysis to prevent type confusion.

[63] There is no longer any definition of the defensive virtual machine in the version 2.6 of the Java Card system protection profile.

5.10.5.1 Description of a partial attack example

The goal of an attack on a defensive virtual machine is to trick the virtual machine in allowing types to be confused. Such an attack may be possible when the defensive virtual machine is implemented only partially.

An ill-formed applet containing byte codes in illegal order is loaded onto the target which then, when defensive checks are not present or incomplete, causes a type confusion. This type confusion can then possibly be used to read persistent and transient data of the JCRE and other contexts not belonging to attacker's context.

A fully fledged type confusion attack uses the type confusion attack itself, the knowledge of the virtual machine meta data, and its application in a single attack applet able to read or write persistent and transient memory.

5.10.5.2 Impact on TOE

The attack is directed against other applications installed on the TOE, or the operating system. The main impacts are:

- Access to secret data of the target applet,
- Modification of applet functions and status

As the internal representation of data is not public the attacker should have critical knowledge of the TOE to interpret the retrieved data, or by experimental analysis on open samples derive the meaning of the data.

5.10.6 Firewall partial attacks

The Java Card Operating System is designed to run all applets in a single virtual machine. It does not have resources to provide a per-application virtual machine, which would provide an isolated runtime environment for each applet. The Java Card firewall is introduced to provide the sandbox environment for applets running in the same virtual machine.

The Java Card firewall limits access to object references by their context. Only objects created within the same context can be referenced. Access to resources outside the context of an object is possible through the Java Card Firewall by means of the Shareable Interface Object mechanism. Static members are excluded from firewall control and their accessibility does not depend on contexts.

5.10.6.1 Description of partial attacks

Malicious applets in the Java Card environment could be used to challenge the restrictions imposed by the Java Card Firewall by attacking the context switching mechanisms. These malicious applets are well-formed and do pass byte-code verification. This attack may be easier to mount then ill-formed applet attacks as a malicious applet attack cannot be detected by byte code verification. On the other hand, this attack can only succeed if the firewall of the TOE is flawed.

5.10.6.2 Impact on TOE

The attack is directed against other applications installed on the TOE, or the operating system. The main impacts are:

- Access to secret data of the target applet,
- Modification of applet functions and status

The potential use of these techniques is specialized and has to be considered in the context of each evaluation. As the internal representation of data is not public the attacker should have critical knowledge of the TOE to interpret the retrieved data, or by experimental analysis on open samples derive the meaning of the data.

5.10.7 Multos partial attacks

MULTOS platform provides a secure environment for application execution and data storage. It is a multi-application operating system enforcing applications segregation. MULTOS applications can be developed in C language, in MULTOS Assembler (MEL) or in Java.

MULTOS does not have a verifier tool for MEL code because this language is less complex. However, MULTOS has similar security mechanisms such as firewall and secure application loading.

MULTOS implements the following countermeasures:

- Instructions, primitives and APDU commands do not allow addresses manipulation. In fact we cannot assign a new address to a variable contrary to Java Card (for instance: aload_1 astore_3)

- The Firewall: applet isolation, code space and data space isolation (for instance, we can't perform a jump from code to data). That's why an application cannot access to another application space and so cannot be accessed by other applications.
- The Application loaded on card can contain:
  - MEL instructions
  - Data
  - DIR record: information about the name of the application when loaded on the card
  - FCI record: information that is returned when a MEL application is selected
  - Application signature (if exist)
  - KTU (if exist)
  - …

It is not possible to manipulate components contrary to Java Card (for instance in order to forge an address by deleting an element in the Reference location).

- The MULTOS Application Abstract Machine provides each application with its own memory space. In fact, the memory space is always relative to the current running application. Tagged addresses are used instead of absolute addresses. This tagged address consists of:
  - A register: ST and SB for static memory, DT, DB and LB for dynamic memory, PB and PT for public memory
  - An offset
  - A different instruction will be generated depending on register used. For instance:
  - Instruction “LOAD SB[1], 0x10” will be “39 10 00 01”.
  - Instruction “LOAD PB[1], 0x10” will be “3E 10 00 01”.
- The Loaded application can be encrypted

5.10.7.1 Description of partial attack

This attack is a combined attack. Its aim is to attempt to read a block of data with an invalid size (a great one) and to perform a fault injection in order to bypass the firewall.

The firewall ensures that an application cannot access to another application space. If the attacker tries to execute an instruction which attempt to read a block of data with an invalid block length, the firewall will detect that the current application attempts to access to other application space and so will return an error. The evaluator needs to perform a fault injection in order to bypass this check and so succeeding to dump a part of memory.

5.10.7.2 Impact on TOE

The main impacts of this attack are:

- Retrieve secret data (such as cryptographic keys),
- Read data/code outside our context.

5.10.8 Full attack path

The full attack paths combines partial attacks to get illegally access to sensitive resources (for example PINs and keys) across applet isolation.

5.10.9 Attacks on memory management (getting a resource from another application)

This attack is the combination of:

1. Getting a memory dump to locate assets and/or sensitive code through physical attacks or software attacks
   The attacker is able through physical perturbation during bytes emission to force the TOE outputting more bytes than expected. The memory dumps obtained, for instance during the ATR or in public APDU commands returning a significant number of bytes, may allow the attacker to identify assets of other applications and their respective addresses in memory.
   It shall be noticed that software attacks such as those described in “**Error! Reference source not found.**” or “**Error! Reference source not found.**” could be used to perform such memory dump instead.

2. Loading an applet through “**Error! Reference source not found.**”.
   The attacker is able through this attack to load a malicious application onto the TOE.

3. Type confusion to manipulate the objects identified in step 2 through “**Error! Reference source not found.**” or “**Error! Reference source not found.**”.

The attacker is able in the malicious applet to illegally manipulate a memory address of an object of another context. In this description, this is achieved through type confusions attacks.

4. Attack on the firewall to execute the getKey method on the object through "**Error! Reference source not found.**".
   The attacker uses physical perturbations to bypass Java Card/Multos Firewall restrictions while manipulating objects out of the legitimate bounds. On a Java Card platform, the malicious applet may illegally invoke the getKey method on an address of an object of another context.

Step 1 and step 2 are used to calibrate the attack. Step 3 and 4 are detailed here because in the partial attacks described in the previous sections, we assume that a single malicious applet can perform every operation whereas in more realistic examples, a malicious applet can only handle its own objects. That's why here a perturbation is used to bypass the firewall restriction.

5.10.9.1 Impact on TOE

Any platform security mechanisms could be bypassed to disclose or alter secrets since security routines (decrypt, update, *etc*) are forced to be legally exercised in a context belonging to the attacked application.

5.10.10 Attacks on code execution (calling a code from another application)

This section describes an attack similar to the previous one but here applied on a non-shared method of another applet.

The same combination of attacks is required, with the following modifications:

1. Getting a memory dump to locate assets and/or sensitive code through physical attacks or software attacks
   Compared to the previous attack, the attacker should not only locate objects (and their respective references) but also reverse part of the code to identify private routines to be called (for instance to reset a security counter or to disable a security mechanism).
2. Loading an applet through "**Error! Reference source not found.**".
   Same as previous attack.
3. Type confusion to manipulate the objects identified in step 2 through "**Error! Reference source not found.**" or "**Error! Reference source not found.**".
   Same as previous attack.
4. Attack on the firewall to execute the getKey method on the object through "**Error! Reference source not found.**".
   The attacker uses physical perturbations to bypass Java Card/Multos Firewall restrictions while manipulating objects out of the legitimate bounds. On a Java Card platform, the malicious applet may illegally invoke an arbitrary method on an address of an object of another context. However, several perturbations may be required to allow invoking a method on an object not owned by the current context through firewall restrictions as during a method execution, object not owned by the current context may be accessed several times, with each time a firewall check[64].

Step 1 and step 2 are used to calibrate the attack. Step 3 and 4 are not recalled here because they are similar compared to the previous attack. It shall be noticed that performing several perturbations is difficult, however still feasible as the firewall check operation can be identified through a synchronisation on the bytecode execution.

5.10.10.1 Impact on TOE

A malicious application may access private routines allowing to reset counters or to deactivate security mechanisms.

[64] In **Error! Reference source not found.**, since getKey is implemented at platform level, there is a great chance that the code is in native language and therefore only a single firewall check should be performed.

APPENDIX A

A.1 Access to TOE factor with respect to package removal

It is the developer’s choice to include or not to include the package (including the integration structure and overall form factor, e.g. stacked die) in the TOE and describe this as such in the Security Target knowing that this would also impact the ALC_DVS class.

Rating for the removal or preparation of the package is expressed in this document in the ‘Access to TOE’ factor (see Section 4.5.1) depending on the effort needed to remove the package. Indeed, the package can be seen as a barrier that prevents an attacker from accessing the TOE to perform physical or invasive attacks.

Details of the three rating levels (Low, Medium, and High preparation effort) are defined in the following section. Please note that package preparation methods and the corresponding assessment difficulty are not seen as mature as other areas like SCA or FI. Therefore, the content of this appendix will be revised if needed.

A.2 Effort levels for TOE package preparation effort

This section describes the current view of the effort required for package removal in more detail.

Low preparation effort:
Simple packages that require low preparation effort and that can be removed by standard chemical etching, mechanical action, re-wiring, or similar for the attack path e.g.:

- Conventional smart cards in most cases,
- Standard plastics like DIP, SOIC, QFP, QFN,..., BGA (targeting the more accessible side, typically back side for flip chip).

Medium preparation effort:
Packages that require medium preparation effort and that have a relatively high risk for fatal damage of the TOE (losing the functionality that is target or required for the evaluation) because of special constructions such as:

- Complex package-on-package with glued interposer board,
- Packages with a passive mesh or obstructive wire bonding: This means that the bonding wires are hard to remove/circumvent or hard to re-wire. For example, it requires significant manual reverse-engineering (>1 week) of several hundred pins to be obtained by generating a bonding map. And, effort to translate the bonding map to a bonding machine file format, for the use of an automated bonding machine. Note that if the reverse-engineering does not need to be redone in exploitation, consequently points in exploitation shall only be given if the remaining attack path still requires specialized equipment or above.
  Separation of the dies can be difficult as there are some functional dependencies in place between the dies, which have to be reconnected involving some reverse engineering, development of a testing device between the dies, and adds risk of putting TOE out of operation,
- Casting compounds, for example based on synthetic material like resin, which require material-specific chemistry, as mechanical removal of the package leads to fatal damage of the TOE with high probability. Such casting compounds are for example used in HSMs (key generation devices in Trust Centres). However, the material specification and state-of-the-art removal methods shall then be subject of the evaluation. The ITSEF should try to remove the package using standard chemical methods, for example a wave of hot fuming sulfuric acid, application of fluoric acid and other.

Note: At this point in time there is no harmonisation between the countries regarding package removal methods and therefore it is a case by case decision/discussion with CB to define what is standard.

High preparation effort:
Packages that require high preparation effort, multiple experts and rare bespoke tooling, which are not claimed as security functionality, such as:

- Chip-on-chip with critical functional dependency that require a wing board to be able to work: It is important to consider methods to circumvent dependencies, e.g. run external memory with lower frequency and

similar. In this example the TOE is not functional without external memory, or the TOE checks presence of the memory, but the SoC adds no protection means for the TOE.
If there are TOE checks for external components, then circumventing these checks matters the evaluation,

- Packages with an active mesh meaning for example that the mesh is connected to the TOE and monitored by the TOE for damages,
- There could be casting compounds, for example on ceramic basis, which cannot be removed without fatal damage of the TOE by using mechanical and also standard chemistry. The removal is therefore either not practical to state-of-the-art-knowledge, as outlined below, or subject to bespoke methods known to the vendor only and shared with the ITSEF in the course of evaluation. I.e. there should be no publicly known method to remove the package material easily or with state-of-the-art chemical methods. For that reason, the material specification and check of the state-of-the-art removal methods shall be subject of the evaluation, which may involve external experts from other faculty, such as chemistry and other. The vendor can also be required to provide material samples for the chemical analysis and attempts. Those material samples can but must not include the TOE.

A.3 Examples for rating the removal of packages

The following package descriptions are not based on existing products and are provided only as examples for the rating methodology:

Example 1

This is the baseline situation where the package does not contribute to the attack resistance. The example assumes a simple Light Fault Injection (e.g. authentication bypass) on a vulnerable TOE in Chip Scale Package or bare die. In this case the effort and skills needed to prepare the TOE for LFI are very limited because CSPs can be easily dissolved by chemical etching. For bare dies no preparation at all is needed.

Table 14: Combined basic laser fault injection and package removal rating for low package preparation effort

LFI on CSP or bare die			
Factors	**Description**	**Identification**	**Exploitation**
Elapsed time	For setting up the equipment and performing the attack an attacker would spend more than a week but less than a month.	< one month (3)	< one week (4)
Expertise	Only proficient knowledge is required with respect to the functionality under attack.	Proficient (2)	Proficient (2)
Knowledge of the TOE	The attack can be performed using public domain information.	Public (0)	Public (0)
Access to TOE	There is no risk the TOE is damaged during opening. So, no points will be given here.	<10 samples (0) **Low preparation effort** **+(0)**	<10 samples (0) **Low preparation effort** **+(0)**
Equipment	Just a standard LFI setup is required. No equipment for package removal.	Specialized (3)	Specialized (4)
Open samples		not required (0)	-
Subtotal		8	10
Total		**18 (Basic)**	

Example 2

Light Fault Injection on a vulnerable TOE in a package-on-package configuration. This is the same TOE as Example 1, but in a different type of package. The vendor claims that the package adds extra security to the TOE. The TOE (bottom package) can work independently from the supporting device inside the top package. The die inside the bottom package is sandwiched between the lower carrier board and upper carrier board. The upper board completely covers the TOE. The voids between the carrier boards are filled with resin. Opening this package requires substantially more time and tools compared to CSPs and bare dies. First the top package must be removed. Then an opening must be made in the upper carrier board without damaging the SoC die inside the bottom package. The SoC die must be exposed for LFI preparation, which requires etching. Finally, the TOE must be fitted inside an LFI set-up and the attack must be performed.

Table 15: Combined basic laser fault injection and package removal rating for medium package preparation effort

LFI on package-on-package without dependency on supporting device (bold text represents the extra resistance provided by package)			
Factors	**Description**	**Identification**	**Exploitation**
Elapsed time	For setting up the equipment and performing the attack an attacker would spend more than a week but less than a month.	< one month (3)	< one week (4)
Expertise	Only proficient knowledge is required with respect to the functionality under attack.	Proficient (2)	Proficient (2)
Knowledge of the TOE	The attack can be performed using public domain information.	Public (0)	Public (0)
Access to TOE	There most likely will be some TOEs destroyed during separation and opening, but not likely more than 10 before successful preparation. **Based on the above de-packaging description it is considered as difficult to prepare (medium effort) the SoC to perform the attack.**	<10 samples (0) **Medium preparation effort** **+(1)**	<10 samples (0) **Medium preparation effort** **+(2)**
Equipment	Just a standard LFI setup is required.	Specialized (3)	Specialized (4)
Open samples		not required (0)	-
Subtotal		9	12
Total		**21 (Enhanced basic)**	

Example 3

Light Fault Injection on a vulnerable TOE in a chip-on-chip package configuration with high data rate interconnections. This is the same TOE as Example 1, but again in a different type of package. These high-speed connections require critical routing to guarantee signal integrity. The chips are glued together which makes separation without damage extremely difficult. The pitch between the contacts is small. Once separated an interface board is required to re-connect both chips. Connecting the interface board to both chips by means of wire bonding is not trivial due to the fine pitch and routing requirements. Further assumptions: Security claim on the package by the developer, upper board completely covers the TOE.

Table 16: Combined basic laser fault injection and package removal rating for high package preparation effort

LFI on chip-on-chip package with dependency on supporting chip (bold text represents the extra resistance provided by package)			
Factors	**Description**	**Identification**	**Exploitation**
Elapsed time	For setting up the equipment and performing the attack an attacker would spend more than a week but less than a month.	< one month (3)	< one week (4)
Expertise	Only proficient knowledge is required with respect to the functionality under attack.	Proficient (2)	Proficient (2)
Knowledge of the TOE	The attack can be performed using public domain information.	Public (0)	Public (0)
Access to TOE	**There most likely will be many TOEs destroyed during separation and opening, especially while figuring out the best approach.** **Based on the de-packaging description it is considered as hard to prepare (high preparation effort) the SoC to perform the attack.**	<10 samples (0) **High preparation effort** **+(2)**	<10 samples (0) **High preparation effort** **+(4)**
Equipment	A standard LFI set-up is required.	Specialized (3)	Specialized (4)
Open samples		not required (0)	-
Subtotal		10	14
Total		**24 (Enhanced Basic)**	

34. ANNEX 8: MINIMUM ITSEF REQUIREMENTS FOR SECURITY EVALUATIONS OF SMART CARDS AND SIMILAR DEVICES

PURPOSE

This annex provides requirements related to the minimum capabilities an accredited ITSEF shall have in its premises to conduct the different types of attacks present in Annex 7, APPLICATION OF ATTACK POTENTIAL TO SMARTCARDS AND SIMILAR DEVICES. These capabilities include the knowledge and the skills of their evaluators and the necessary equipment, and evaluation methodology description, all necessary to conduct the attacks mentioned above.

The capabilities are intended to cover the minimum requirements to perform the evaluation of an Integrated Circuit (IC), a crypto library, a platform, and Integrated Circuit Card (ICC) with sufficient guarantees.

This annex is not intended to provide guidance on how an IC, crypto library, platform (IC + OS) or ICC (IC + OS + App) evaluation has to be performed, but it provides guidance to ensure ITSEFs have the necessary capabilities to conduct such evaluations.

PARTICULAR STATUS

None.

CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE

Chapter 6, SPECIFIC REQUIREMENTS APPLICABLE TO A CAB
Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS.

1 REQUIRED CAPABILITIES FOR IC EVALUATIONS

1.1 Overview for an IC evaluation

An IC evaluation requires the development of specific skills and knowledge. The aim is to provide a technical guidance for evaluators running an IC evaluation and to expose the related minimum requirements. To achieve this, the following sections will encompass:

- The understanding of secure IC-based design (such as smartcard, secure element, etc.) and production process in general of the IC design and manufacturing process (refer to section 1.2).
- The understanding of secure IC technology, its underlying principles and the development equipment used by secure IC manufacturers (refer to section 1.3).
- The knowledge and experience in hardware physical attack techniques that could compromise a secure IC and an ability to use the related equipment to stress the hardware layers. This includes the understanding of the IC underlying physical principles (refer to section 1.4).
- The knowledge and experience in physical disruptions that could change the secure IC behaviour, with the aim to subsequently downgrade the security of the IC-based device. The ability to use related equipment to conduct physical disruptions and the understanding of related physical effects on the hardware (refer to section 1.4).
- The knowledge and experience in cryptographic attack techniques and the ability to perform the analysis (including data-capture and signal processing procedures) (refer to section 1.4).

1.2 IC Design and Production Process

IC hardware and software are in general developed by different companies. These components are then integrated and additional security relevant data is injected into the card.

The security objectives for an IC are twofold:

- Ensure a level of security for the card in the field.
- Maintain the level of security throughout the development and production process.

Although many specialists concentrate on security in the field (since the smartcard is delivered into a hostile, unregulated environment and may be subject to tampering), security during the development, production and personalization process is also important. The security objectives that a smartcard component is assessed against depend very much on the application context, which in turn can be dependent upon the production and personalization process. In particular, personalization affects the security functionality to be provided by the smartcard.

The CEM depicts an ideal development process starting with a definition of requirements followed by the design process, implementation, testing, acceptance, delivery and usage. When looking at the components of a composite product this process must be interpreted and rearranged.

For instance, the chip manufacturer develops the design of the chip hardware and software for testing. He receives the software from the software developer to create the ROM image. Then the mask files are sent to the mask manufacturer. The masks or reticles are returned to the chip manufacturer. After wafer production the chips are tested and initialisation data (transport keys, traceability data) are injected into the EEPROM (or other non-volatile memory). The initialisation data is defined by the card manufacturer. Operational dies are delivered or directly embedded into modules. The protection of die delivery can be complex. The authentication mechanism is realised by the software manufacturer but used by the card manufacturer (or personalisation centre). The keys are generated by the card manufacturer and injected into the card by the chip manufacturer using a procedure (for diversification etc.) defined by the card manufacturer.

In case of flash based ICs there are even more possibilities. The IC can be delivered either without any content at all, which requires the software developer to use the test interface to initialise the flash with the firmware, boot loader or with bootloader software, hardware drivers or even with an operating system. In any case, proper use of authentication mechanisms must make sure the integrity of the flash content and access to the download functionality of the IC is handled in a secure fashion.

These examples show that a real development process can be more complex than the assumed one by the CEM for conventional software or hardware products, since the complete life-cycle of a smartcard can be quite complex. Inputs and outputs are not always as simple as expected by the CEM. As a result, the corresponding assurance components of the CEM (for instance delivery) must be interpreted, refined, and rearranged as required. In addition, it must ensure the processes of different components (and their description in terms of Common Criteria assurance components) fit together.

The evaluator must understand the smartcard supply chain and its integration into the application context in order to interpret the CEM assurance requirements in an appropriate way. In particular, these assurance requirements are:

- Guidance
- Delivery
- Preparation procedures
- Tools and Techniques
- Life-Cycle Definition
- Development Security

In addition, differences between the evaluation of smartcard ICs and the evaluation of software means the interpretation of the CC Part 3 assurance components of the classes ASE, ADV, ATE, and AVA are also required.

These interpretations of the CC Part 3 assurance components and additional guidance are described in several EUCC supporting documents for smartcards and similar devices that are published on the ENISA website dedicated to cybersecurity certification.

1.3 Smartcard Integrated Circuit Technology

The evaluator must understand smartcard integrated circuit technology and the underlying principles to the extent necessary to comprehend the design decisions of the IC manufacturer. Basic knowledge is required of:

- Electron theory of semiconductors (physics) and the electrical behaviour of semiconductors and transistors.
- Physical and electrical behaviour of all standard materials used in integrated circuit manufacturing (for instance silicon, poly-silicon, metal, and isolating and passivation material).
- Production steps and the resulting layer structure on the chip's surface.

In addition, the evaluator must have detailed knowledge of:

- Physical layout (implementation on the semiconductor surface) of standard cells (simple gates), memory cells (E2PROM, RAM, ROM) and memory blocks.
- Layout principles and methods of routing and layering.
- Digital and analogue circuit engineering (digital gates of different complexity and standard analogue circuitry).
- Static and dynamic behaviour of digital and analogue circuitry.
- Microcontroller architecture and functionality.
- Realisation of standard circuitry as used in micro-controllers.

The evaluator must be able to understand the schematics (block diagrams, schematics on gate and transistor level). The functional components can be described in the form of standard schematics or in VHDL sources.

The evaluator must have knowledge of the VLSI design process and must understand the process from the schematics or VHDL sources (logical representation of the chip) to the actual layout and dice/wafers (physical representation). The evaluator must understand the processes of technology qualification, functional testing, characterisation, and reliability testing.

The evaluator must understand the development equipment used by the manufacturers for micro-controller software. This includes simulators, emulators, protocol analysers and special evaluation software masks. The evaluator must be able to read micro-controller source code and to develop software for penetration testing and other investigations. Therefore, the evaluator must understand the CPU instruction set, the memory map and use of other peripheral units of the micro-controller.

1.4 Smartcard Specific Attacks

The following provides an overview about smartcard specific attacks. This is not a complete list but provides some examples. More detailed information about smartcard specific attacks in the context of CC-based evaluation can be found in Annex 7, APPLICATION OF ATTACK POTENTIAL TO SMARTCARDS AND SIMILAR DEVICES,

The evaluator must have knowledge of standard smartcard fraud and attack scenarios and in principle be able to develop new ideas for such attacks. To be more specific, the evaluator must know about attack scenarios for ICs and smartcard software such as physical manipulation and probing, malfunction attacks, inherent and forced leakage attacks, abuse of test features, attacks on the implementation of cryptographic functionality implemented in hardware, software or in a combination of both, cryptographic attacks or software attacks. A multitude of such attack scenarios – along with quotations – is described in the Annex cited above.

The evaluator must be able to adapt and combine these attack scenarios for the individual chip or smartcard being subject to evaluation. During the vulnerability analysis, the evaluator must be able to find possible weaknesses (in schematics and their realisation on the chip and the combination thereof) and be able to use the standard techniques to assess them.

The evaluator must have knowledge and experience in IC failure analysis to be used for physical manipulation and probing. The evaluator must at least understand the physical principles of this and be able to operate (as appropriate) the equipment classified as 'standard' and 'specialised'. Moreover, the evaluator must be able to use the 'bespoke' tools with the help of trained operators. The evaluator must know how these tools and techniques can be used during vulnerability analysis in order to assess the IC's security properties and functions. The method and purpose of using the equipment (especially Focused Ion Beam (FIB), Scanning Electron Microscope (SEM), EMMI or E-beam Tester) during the vulnerability assessment need not necessarily correspond to the expectations of the operating personnel. The evaluator should instruct the operating personnel in order to achieve a meaningful and independent evaluation. The evaluator himself shall maintain sufficient technical knowledge (for instance on how to operate IC failure analysis equipment), required for a meaningful instruction.

The evaluator must have sufficient knowledge in probability theory and design principles of RNGs. The evaluator must be able to identify and analyse those characteristics of a system or a process that have significant impact on the distribution of random numbers and to rate the randomness of number generation.

The evaluator must have knowledge and experience of other smartcard attacks (side channel attacks such as Timing Analysis, Differential Power Analysis (DPA), Differential EM radiation Analysis (DEMA), Template Attacks (TA); fault injection attacks such as DFA and related attacks) and possess the equipment (physical and analysis tools) necessary to perform such attacks. The evaluator must be able to operate this equipment (including data-capture procedures) and to perform the analysis (mathematics). Knowledge and experience in cryptography and standard cryptographic attack techniques for all type of algorithms involved is required. The underlying principles of side channel attacks as well as fault injection attacks (such as Differential Fault Analysis (DFA) and other attacks) must be fundamentally understood. In order to fully investigate for potential weaknesses, the evaluator must be able to detect vulnerabilities related to such attacks, encompassing EM emission analysis, single- and multi-laser attacks, etc.

The evaluator must be able to develop software to communicate with the smartcard. Therefore, the evaluator must understand the I/O protocol being supported, the operating conditions and the external command interface if being used or attacked. The evaluator must also understand the security concepts of smartcard software, including file structures, encoding of access rights, etc.

The evaluator must know how to handle chip card readers and be able to modify them in order to use the chips in different packages and to apply non-standard operating conditions. Therefore, the evaluator must be able to use standard equipment such as voltage supply, signal and function generators, oscilloscopes, and soldering irons. In addition, the evaluator shall know how to physically prepare samples (e.g. open package and remove metal layers); for instance to facilitate sophisticated light attacks or EM measurements, provide laser access, enable FIB probing, allow reverse engineering, etc.

The evaluator must be able to combine results of different capabilities described above. This comprises the application of failure analysis methods to localise components on smartcards in order to assess if design data can be substituted or to judge the effectiveness of different attack methods with the same target.

1.5 Equipment for IC evaluation

In order to accomplish the vulnerability analysis, physical manipulations and attack scenarios mentioned in section 1.4, the ITSEF must have unlimited access to, and own the majority of the tools necessary to perform those attacks and shall be able to use them efficiently. Categories of this equipment are listed below (Annex 7, APPLICATION OF ATTACK POTENTIAL TO SMARTCARDS AND SIMILAR DEVICES provides further details on necessary equipment with their categorisation.):

- Environment control equipment (e.g. to control communication, voltage, clock, and temperature)
- Chemical and mechanical lab equipment (i.e. for sample preparation and analysis)
- Imaging equipment (e.g. cameras, microscopes, SEM)
- Physical manipulation equipment (e.g. probe station, Focused Ion Beam)
- Design analysis tools (e.g. for chip layout analysis, RNG analysis)
- Protocol analysers (e.g., spy devices)
- Logical test tools (e.g. for interface testing, vulnerability scanning)
- Side Channel Analysis equipment (e.g. probes, oscilloscopes, analysis software)
- Perturbation equipment (e.g. pulse generators, lasers, smart triggering)

For the equipment categorised as 'bespoke', the evaluator must have a good understanding of the underlying physical principles and of the capabilities of the tools.

The tools shall allow flexible usage within their technical limits. The usage shall not be limited to the expectations of the operating personnel as already described in section 1.4. The tools shall enable the evaluator to customise attacks as it can be assumed for experts based on the implementation under assessment.

2 REQUIRED CAPABILITIES FOR COMPOSITE EVALUATIONS

Composite evaluations build upon an earlier certified product. The composite TOE could be the IC supplemented by a crypto library, a platform, or the full ICC including the application. Typically, the TOE concerns software added to the certified underlying product.

2.1 Overview for an IC Card Operating System

2.1.1 Source Code Review

Currently, most smartcard software is written in the programming language C, followed by Java; while manual programming in Assembler language is rather seldom today (except for dedicated core routines). The evaluator needs a thorough understanding of the use of C or Java in the context of the specific hardware architecture and constraints of a smartcard IC; this refers especially to the constraints of Java for Java Card products. (Therefore, section 2.4 below is dedicated to Virtual Machines.)

Moreover, for an in-depth security analysis, an understanding of assembler code and intermediate code (like Java Card byte code) is required. In particular, a variety of security impacts (and defects) cannot be understood on the level of a higher language like C or Java, because they become only apparent in Assembler Code or byte code. Therefore, the importance of understanding Assembler Code produced by a compiler and security impacts of generation tools shall be explicitly emphasized.

2.1.2 Native I/O

Native I/O refers to technologies “at the bottom” of data transfer between a smartcard and a terminal (smartcard reader).

The evaluator needs to understand and be able to interpret different I/O layers ranging from basic interface specification like UART (for sending and receiving single bytes); over the basic command structure of smartcard commands (APDU – Application Protocol Data Unit); up to the level of commonly used data exchange protocols, e.g. (T0 / T1 for contact, and TCL / Single Wire Protocol (SWP) for contactless.

2.1.3 (Security) Protocol I/O

In contrast to Native I/O, Protocol I/O encompasses the security (mostly cryptographic) protocols employed in communication with a smartcard.

In the context of smartcard protocols, Secure Messaging is the term which comprises security features of data transmission between a smartcard and a terminal (or a remote server). Secure Messaging may include mutual or one-sided authentication between a smartcard and a host, message integrity, as well as confidentiality of messages.

The evaluator must understand the various standardized protocols that exist for Secure Messaging, like specified for Open Platform, ECC (European Citizen Card), BAC (Basic Access Control), PACE (Password Authenticated Connection Establishment), EAC (Extended Access Control), etc. Often these standards allow a high degree of flexibility in the configuration of security options, demanding scrutiny when evaluating a specific choice against a set of prerequisite requirements.

2.1.4 Content and Resource Management

The defining task of an operating system is the management of computational resources (like memory, RAM, I/O etc.) and the administration of access (interface) to such resources.

While the previous paragraphs dealt with the communication between a smartcard and the outside world, the focus shall lie here on the resource management inside the smartcard itself.

The evaluator first needs to understand the file structure (e.g. the hierarchy concept of Master Files, Dedicated Files and Elementary Files) and file access rights administration within a smartcard’s operating system. Knowledge of the memory types (EE, Flash, ROM, RAM, special dedicated RAM (like Crypto-RAM, Buffer-RAM)) and memory management procedures (e.g. access limitations) are required.

For Java Cards, the concept of Security Domains and Application Isolation (formerly firewalling) needs to be profoundly understood. This is especially relevant for application management, which refers to the secure loading, administration, and deletion of application, as well as the access rights of such applications to the smartcard’s resources.

2.2 IC Card production cycle process

An IC Card is produced by a software developer based on an IC or platform of a (different) vendor. The software for the IC is called the embedded software.

The security objectives for an IC Card are twofold:

- Ensure a level of security for the IC Card in the field.
- Maintain the level of security throughout the development and production process.

Although many specialists concentrate on security in the field (since the IC card is delivered into a hostile, unregulated environment and may be subject to tampering), security during the development, production and personalization process is also important. The security objectives that a smartcard component is assessed against will depend very much on the application context, which can be dependent upon the production and personalization process. In particular, personalization affects the security functionality to be provided by the smartcard.

The CEM depicts an ideal development process starting with a definition of the requirements, followed by the design process, implementation, test, acceptance, delivery and usage. When looking at the components of a composite product this process must be interpreted and rearranged.

For instance, the embedded software is developed for a specific IC. The IC has undergone a hardware evaluation and provides security guidance documents in order to make the composite product secure. These guidance documents include information on how the IC must be used to make the IC Card a secure product – usually several items of information are included, ranging from secure use of the cryptographic components, the Random Number Generator and a secure boot procedure. The composite evaluator must therefore understand the importance of the mandatory IC (security) guidance documents. It must be assessed whether the security mechanisms that have been implemented in the embedded software fulfil the requirements mentioned in the (security) guidance documents.

When assembling the IC Card, several entities are involved. For ROM based ICs, the embedded software will be sent to the IC manufacturer, whereas for flash based ICs, software loading could be done by the embedded software developer or even a third party. After assembling the IC Card, it will be made ready for delivery to the final customer or personalization bureau by the software developer. This may involve pre-personalisation of the IC Card and applications. These processes typically involve protection by cryptographic operations. The composite evaluator must understand how all these security mechanisms are implemented to guarantee a secure IC Card production process (including personalization).

The embedded software developer may introduce security mechanisms for changing the behaviour of the IC Card, for example by patching mechanism. The patch mechanism allows loading new (potentially malicious) program code to the IC Card and requires authentication before a patch can be applied. The composite evaluator must be able to assess the security mechanisms involved in such a patch mechanism.

These examples show that a real development process can be more complex than the one assumed by the CEM for conventional software or hardware products, since the complete life-cycle of a smartcard can be quite complex. This life cycle involves several “players” such as the IC manufacturer, the Software Embedder, the Card Issuer (who usually remains the legal card owner even after card issuance), Application Providers, and the End Users (the “card holders”). Inputs and outputs are not always as simple as expected by the CEM, since there is a complex interaction between the aforementioned entities with regard to security relevant procedures such as code exchange, key administration, or applet loading. As a result, the corresponding assurance components of the CEM (for instance delivery) must be interpreted, refined, and rearranged if needed. In addition, it must be ensured that the processes of different components (and their description in terms of the CC Part 3 assurance components) fit together.

The evaluator must understand the smartcard supply chain and its integration into the application context in order to be able to interpret the CC Part 3 assurance requirements in an appropriate way. In particular, these assurance requirements are:

- Guidance,
- Delivery,
- Preparation procedures,
- Tools and Techniques,
- Life-Cycle Definition,
- Development Security.

In addition, differences between the evaluation of smartcard ICs and the evaluation of software means that the interpretation of the Common Criteria assurance components of the classes ASE, ADV, ATE, and AVA is also required.

These interpretations of the CC Part 3 assurance components and additional guidance are described in several EUCC Supporting Documents for Smartcards and similar devices that are published on the ENISA website dedicated to cybersecurity certification.

2.3 Cryptographic software

Composite products may include (partial) software implementations of cryptographic algorithms. In addition to understanding the algorithms, the evaluator should also understand interaction aspects between software and hardware, and the effect of attacks on a software implementation.

2.3.1 Cryptographic library using a cryptographic coprocessor

This section covers typically asymmetric cryptography using crypto coprocessor such as RSA, ECC, but could also concern symmetric algorithms lying on a cryptographic accelerator.

Such implementations combine a software-based algorithm with a dedicated set of cryptographic features. Both fit closely together because of the nature of the cryptographic accelerator. The evaluator shall be able to identify weaknesses in the interaction between hardware and software.

There is a significant variety of different implementation of hardware-accelerated algorithms, particularly when it comes to big integer operations. As a result, a good knowledge of the different implementations and a strong algebraic and arithmetic mathematical background is necessary.

In addition, a large number of attack paths may compromise the algorithms and many of them are implementation-specific. Therefore, it is of high importance that the evaluator has strong knowledge of attacks and countermeasures to provide an in-depth analysis of the embedded cryptographic library.

Furthermore, the evaluator will not be able to assume a specific usage of the algorithm at this stage of the assessment. For instance, the format of the input data must remain agnostic. Therefore, the evaluator needs to take into account various scenarios encompassing the most representative cryptographic protocols potentially relying on the cryptographic algorithms.

2.3.2 Cryptographic software without dedicated hardware (HW) support

Different secret key implementation without any HW support or with a partial HW support can be found in several products. Such software implementations can involve several countermeasures like random permutations, dummy operations or random masking as depicted in various publications to protect the product against first and higher order side-channel attacks. It is also very important to analyse the key bit (bytes) manipulations that must protect against other statistical attacks like template attacks.

It is very important the evaluator has strong knowledge in the different side-channel and fault attack techniques that can defeat all these countermeasures if they are not strong enough nor properly implemented.

The evaluator shall understand the algorithms that fall in the evaluation scope of the TOE. We can list the following cases of software implemented algorithms that are frequently met in products:

- “stand-alone” implementation of AES, DES (in spite of existing HW support still SW implementations are used) can be used. The whole implementation is done in software which relies on the set of instructions provided by the IC core (CPU).
- Mixed software/hardware implementation of DES and AES where additional software and countermeasures are required to the accelerations offered by the HW.
- Implementation of algorithms for which usually no HW support on smartcard IC exists, like:
    - Hash algorithms: Sha1, Sha2, Sha3, Ripemd160, Md5, etc…
    - Various authentication algorithms for mobile networks (Milenage, TUAK; moreover, a multitude of proprietary algorithms).
    - Other secret key algorithms from different NIST or national scheme standards.

2.4 Virtual Machine

A virtual machine, by definition, is a software implementation of a computing environment in which an operating system or program can be installed and run. An evaluator must understand how the virtual machine and the run time environment works and protects the security assets relying on the platform. Different basic knowledge and skills are required:

- Generic knowledge and experience on interpreted languages, such as Java Card, with specific knowledge on the virtual machine architecture and parts, supported instruction set and data types and structures.

- Knowledge on the different programming languages used for the native parts and interpreter implementation (lower layers) and also for the applications (upper layers).
- Knowledge and experience with the development process and involved tools for the different platform parts are required. Compilers, converters and simulators, as well as, their associated intermediate and final file types and configurations, are required to be known.

2.4.1 Runtime environment

Evaluators must understand how the Runtime Environment (RE) ensures the security model of the virtual platform is upheld. This comprehends a deep knowledge on the relationship and interactions between RE, operating system, applications and hardware, the RE lifetime and transaction mechanisms, how the RE allows application isolation and data sharing mechanisms and how the applications are loaded and managed are part of the RE core knowledge that is required to be deeply comprehended.

2.4.2 Application Programming Interface

An Application Programming Interface (API) defines a set of services which are available for the application developers and provide system services, such as application management, transaction management, communications or cryptographic functionality. Evaluators must know the scope of the API services and how applications access RE services and their security implications. API services for Card Holder Verification, card content management or cryptographic operations are examples of critical services which evaluators must have very specific understanding. It is also required to be able to develop and use the different provided API's in order to develop security testing applications.

2.5 Attacks

In the following a short overview of typical attacks that need to be considered for composite evaluations will be given. A more complete list is provided by Annex 7, APPLICATION OF ATTACK POTENTIAL TO SMARTCARDS AND SIMILAR DEVICES. There is a large overlap with section 1.4 dedicated to IC evaluations but the focus is now on the embedded software to be added by the composite evaluation and the interplay between the already certified part(s) and the new software.

Typically, some additional hardware attacks need to be performed, although the hardware belongs to the already certified part: The evaluator will need to ascertain through side channel measurements and fault injection attacks that the software correctly utilises hardware protection features and adds additional protection when necessary. For example, it could be required to configure registers in a particular way, interpret attack attempts reported by the hardware properly or implement software counter-measures for increased side channel or fault injection resistance. It must be ensured that the TOE as a whole maintains the required security level and the evaluator must also consider the purpose, use cases and frequency of use of the cryptographic keys, algorithms, and secret data stored in the TOE. The knowledge required to perform these attacks is identical to what is described in the corresponding paragraph in section 1.4.

Another topic that is concerned with the correct interplay of hardware and software is attacks on the random number generator. Again, correct use of a hardware TRNG and additional software measures such as post processing and on-line testing of random numbers must be verified. Attack methods include hardware attacks such as fault injection and software tools such as statistical analysis.

Primarily, the evaluator concentrates on the embedded software implemented on top of the already certified part. The embedded software can be very complex and the evaluator must develop a good understanding of its architecture, the interfaces, and protocols used for external communication, as well as the assets it is intended to protect. The evaluator must be able to review code, while tracing the use of assets and identifying vulnerabilities.

When attacking the software implementation from external interfaces, it is crucial the evaluator is able to communicate with the TOE, send arbitrary commands and exercise all life-cycle states. The evaluator will have knowledge of software debugging tools and in order to operate them efficiently, the evaluator must have knowledge of the programming language used for implementation, the assembly instructions available on the CPU and the functionality of a debugger (breakpoints, memory inspection). A supporting technique is to apply automated tools to the source code, which perform a static analysis. The evaluator must be able to interpret and judge the results.

Additionally, some TOEs such as Java Cards may allow the installation of additional software such as applets. If that is the case, the evaluator must be able to load additional applets onto the card. Good programming skills are required in this case and precise knowledge of the internal separation mechanisms of the TOE such as firewalls, memory management, and bytecode verification.

Based on his knowledge about the TOE and the technical abilities described in the previous paragraphs, the evaluator must develop attack scenarios aiming at revealing sensitive assets or circumventing the intended security functionality of the TOE. These can be logical attacks (e.g. side effects or unintended effects of legal commands and API functions, malformed commands, parameters, or confusion of the internal state of the TOE) on the available interfaces or a combination of logical and hardware attacks (such as fault injection). A broad range of attack ideas is given in Annex 7, APPLICATION OF ATTACK POTENTIAL TO SMARTCARDS AND SIMILAR DEVICES.

In addition, the evaluator must develop new attacks or modify and adapt standard attacks to assess the specific implementation of the current TOE. In order to be successful, the evaluator must perform a careful vulnerability analysis and have good knowledge of all technologies described in section 2.1 to 2.4 of this chapter and possible attacks against them.

2.6 Equipment for a composite evaluation

For the composite evaluation, use bespoke failure analysis equipment is not expected since the intrinsic resistance of the TOE against physical attacks has already been investigated during the IC evaluation and these kind of attacks are not influenced by the embedded software. On the other hand, most of the IC exhibits some remaining leakages or fault sensitivities that could be exploited by an attacker if the embedded software does not implement additional countermeasures. Finally, software attacks and combined attacks can only be investigated during composite evaluation since they are fully linked to the embedded software.

So in order to be able to evaluate the resistance of the final product the ITSEF must have unlimited access to equipment and tools that can be used to operate the above mentioned class of attacks. The categories of required equipment include:

- Environment control equipment (e.g. to control communication, voltage, clock, and temperature)
- Chemical and mechanical lab equipment (i.e. for sample preparation and analysis)
- Imaging equipment (e.g. cameras, microscopes)
- Logical test tools (e.g. for interface testing, vulnerability scanning, operating system testing, randomness analysis)
- Protocol analysers (e.g., spy devices)
- Side Channel Analysis equipment (e.g. probes, oscilloscopes, analysis software)
- Perturbation equipment (e.g. pulse generators, lasers, smart triggering)

For in depth analysis, it appears necessary to have tools with enough flexibility to customise the attacks in line with the implementation under assessment. This includes the combination of tools (test benches) described above.

35. ANNEX 9: APPLICATION OF ATTACK POTENTIAL TO HARDWARE DEVICES WITH SECURITY BOXES

PURPOSE

This annex contains descriptions of attack methods that are specific for hardware devices with security boxes and provides guidance metrics to calculate the attack potential required by an attacker to effect an attack. The underlying objective is to aid in expressing the total effort required to mount a successful attack applied to the operational behaviour of a hardware device with a security box.

PARTICULAR STATUS

None.

CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE

Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS.

1 INTRODUCTION

This annex contains descriptions of attack methods that are specific for hardware devices with security boxes and provides guidance metrics to calculate the attack potential required by an attacker to effect an attack. The underlying objective is to aid in expressing the total effort required to mount a successful attack applied to the operational behaviour of a hardware device with a security box.

For each of the attacks, the attack potential rating is analysed according to the tables included in section 2, Parameters conditioning attacks.

NOTE: further analysis is to be detailed providing ratings for specific real cases and taking into account possible countermeasures implemented to mitigate the attacks.

2 PARAMETERS CONDITIONING ATTACKS

2.1 Scale factor

The size is one of the factors conditioning the attacks to be performed against devices with security boxes. Depending on the scale of the device, the attack could be different, and the difficulty may increase or decrease depending on such scale.

A size categorization can be made in the following manner.

2.1.1 Macroscopic scale

This scale surrounds the attacks performed against entire devices with its complete external enclosure. The enclosure may have several components inside, such as PCB boards, batteries, etc., so that the aim of the attack is gain access to the internal parts of the enclosure.

2.1.2 Micro- technology

In this case, the scale surrounds the attacks performed against assembled electronic components, such as PCB boards containing buses and ICs. The attacks can be made against the buses transmitting data between components, or perhaps against the IC connectors.

2.1.3 Nano-technology

This scale contemplates the internals of the ICs. Very precise and specialized tools are needed to perform attacks against the ICs internals. These attacks could have the aim of modifying the IC behaviour, or obtain data stored within the IC.

2.2 Factors for the attack potential calculation

Note about the Common Criteria (CC): The CC do no introduce any distinction between the identification phase and the exploitation phase. But considering Security Boxes, the risk management performed by the user of CC certificates required clearly to have a distinction between the cost of “identification” (definition of the attack) and the cost of “exploitation” (e.g. once a script is published). Therefore this distinction is kept when calculating attack potential for Security Boxes evaluation. Although the distinction between identification and exploitation is essential for the evaluation of a Security Box to understand and document the attack path, the final sum of attack potential will be calculated by adding the points of the two phases, as both phases build the complete attack.

2.2.1 How to compute an attack

Attack path identification and exploitation analysis and tests are mapped to relevant factors: attack time, expertise, knowledge of the Security Box, access to the TOE per unit required for the attack, equipment required, or the required window of opportunity to execute the attack.

Even if the attack consists of several steps, the identification and exploitation rating need only be computed for the entire attack path. It is not allowed to calculate the rating for each step separately and to sum up the points afterwards since in that case different factors would count multiple (e.g. tools and expertise). An entire attack path or full attack starts with the preparation activities for an attack and ends when the attacker could gain access to a TOE asset. A full attack does not end with a violation of a SFR if access to a TOE asset could not be gained.

The identification part of an attack corresponds to the effort required to create the attack, and to demonstrate that it can be successfully applied to the TOE (including setting up or building any necessary test equipment). The demonstration that the attack can be successfully applied needs to consider any difficulties in expanding a result shown in the laboratory to create a useful attack. It may not be necessary to carry out all of the experiments to identify the full attack, but to provide that it is clear whether the attack actually proves that access has been gained to a TOE asset, and that the complete attack could realistically be carried out. One of the outputs from the Identification phase assumes a script giving a step-by-step description of how to carry out the attack – this script is assumed to be used in the exploitation part.

Sometimes the identification phase will involve the development of a new type of attack (possibly involving the creation of new equipment) which can subsequently be applied to other TOEs. In such a case the question arises as to how to handle the elapsed time and other parameters when the attack is reapplied. The interpretation taken in this annex is that the development time (and, if relevant, expertise) for identification will include the development time for the initial creation of the attack until a point determined by the relevant Certification Body. Once a Certification Body has determined this point, then no rating points for the development of the attack (in terms of time or expertise) can be used in the attack potential calculation.

The exploitation part of an attack corresponds to achieving the attack on another instance of the TOE using the analysis and techniques defined in the identification part of an attack. It is assumed that a different attacker carries out the exploitation, but that the technique (and relevant background information) is available for the exploitation in the form of a script or set of instructions defined during the identification of the attack. The script is assumed to identify the necessary equipment. This means that the elapsed time, expertise and TOE knowledge ratings for exploitation will sometimes be lower for exploitation than for identification.

In many cases, the evaluators will estimate the parameters for the exploitation phase, rather than carry out the full exploitation. The estimates and their rationale will be documented in the ETR.

To complete an attack potential calculation. the rating points for identification and exploitation have to be added as both phases build the complete attack. When presenting the attack potential calculation in the ETR, the evaluators will make an argument for the appropriateness of the parameter values used, and will therefore give the developer a chance to challenge the calculation before certification. The final attack potential result will therefore be based on discussions between the developer, the ITSEF and the CB, with the CB making the final decision if agreement cannot be reached.

2.2.2 Elapsed time

The Elapsed Time is calculated in hours taken by an attacker to identify or exploit an attack. Time is divided into the following intervals:

Table 6: Rating for Elapsed Time

Elapsed Time	Identification	Exploitation
< one hour	0	0
≤ one day	1	2
≤ one week	2	3
≤ one month	3	4
> one month	5	7

For purposes of calculating time, a day = 8 hours; a week = 40 hours; and a month = 180 hours.

If the attack consists of several steps, the Elapsed Time can be determined and added to achieve a total Elapsed Time for each of these steps. Actual labour time has to be used instead of time expired as long as there is not a minimum Elapsed Time enforced by the attack method applied (for instance, the time needed for performing a side channel analysis or the time needed for an epoxy to harden). In those cases, where attendance is not required during part of the Elapsed Time, the Elapsed Time has to be taken as expired time divided by 3. The idea behind the division by three is that e.g. a computer is able to work 24 hours per day, not only 8 hours per day.

2.2.3 Expertise

Expertise refers to the level of generic knowledge and skills in the application area or product type (e.g. microelectronics, chemistry, skills handling specific drills). For the purpose of Security Boxes three types of experts are defined:

- Laymen are unknowledgeable compared to experts or proficient persons, with no particular expertise or skills in the area.
- Proficient persons are knowledgeable in that they are familiar with the security behaviour of the product, or they have certain (amateur level) expertise handling specific machines or attack techniques to security boxes.
- Experts have a professional experience with specific machines (handling and configuring), security box hardware structures, materials, etc. implemented in the product or system type and the principles and concepts of security employed.

Expertise necessary to carry out an attack may cover several disciplines: chemical, ability to drive sophisticated tools, etc.

Table 7: Definition of Expertise

	Definition according to CEM	Detailed definition to be used in Security Boxes
Experts	Familiar with implemented -Algorithms -Protocol -Hardware structures -Principles and concepts of security.	Professional experience with -Security boxes hardware structures -Configuration and handling of specific equipment (milling/drills, x-rays,) -Electronic and microelectronic knowledge (sensors, actuators, etc.). and -Techniques and tools for the definition of new attacks.
Proficient	Familiar with -security behaviour	Familiar with -security behaviour and classical attacks to security boxes.
Laymen	No particular expertise	No particular expertise

Table 8: Extent of expertise

Extent of expertise **(in order of spread of equipment or TOE knowledge)**	
Equipment: The level of expertise depends on the degree to which tools require experience to drive them: • Milling machines • Drilling machines • CNC milling machines • X-ray machines • Lasers • Optical Microscope • Chemistry (etching, grinding) • [..]	**Knowledge:** The level of expertise depends on skills and knowledge of: • Common Security boxes information • TOE specific hardware structures • Principles and concepts of security • Destructive/ Non-destructive Techniques. • Microelectronics (sensor types and technologies) • [..]

It may occur that for sophisticated attacks, several types of expertise are required. In such cases, the higher of the different expertise factors is chosen.

A new level “Multiple Expert” was introduced to allow for a situation, where different fields of expertise are required at an Expert level for distinct steps of an attack. It should be noted that the expertise must concern fields that are strictly different like for example HW and machines manipulation and microelectronics or chemistry.

Table 9: Rating for Expertise

	Identification	Exploitation
Layman	0	0
Proficient	1	1
Expert	2	3
Multiple Expert	5	6

2.2.4 Knowledge of TOE

The CEM states “to require sensitive information for exploitation would be unusual”, however it shall be clearly understood that any information required for identification shall not be considered as an additional factor for the exploitation.

Since all sensitive and critical design information must be well controlled and protected by the developer, it may not be obvious how it assists in determining a dedicated attack path. Therefore, it shall be clearly stated in the attack potential calculation why the required critical information cannot be substituted by a related combination of time and expertise, e.g. a planning ingredient for a dedicated attack.

The following classification is to be used:

- **Public information** about the TOE (or no information): Information is considered public if it can be easily obtained by anyone (e.g., from the Internet) or if it is provided by the vendor to any customer.
- **Restricted information** concerning the TOE (e.g., as gained from vendor technical specifications): Information is considered restricted if it is distributed on request and the distribution is registered. Suitable example might be the functional specification (ADV_FSP).
- **Sensitive information** about the TOE (e.g., knowledge of internal design, which may have to be obtained by “social engineering” or exhaustive reverse engineering). Suitable example might be High-Level Design (HLD), Low- Level-Design (LLD) information.

Care should be taken here to distinguish between information required to identify the vulnerability and the information required to exploit it, especially in the area of sensitive information. Requiring sensitive information for exploitation would be unusual.

It may occur that for sophisticated attacks, several types of knowledge are required. In such cases, the higher of the different knowledge factors is chosen.

Table 10: Rating for Knowledge of TOE

Knowledge	Identification	Exploitation
Public	0	0
Restricted	2	2
Sensitive	3	4

Note: Specialist expertise and knowledge of the TOE are concerned with the information required for persons to be able to attack a TOE. There is an implicit relationship between an attacker's expertise and the ability to effectively make use of equipment in an attack. The weaker the attacker's expertise, the lower the potential to effectively use equipment. Likewise, the greater the expertise, the greater the potential for equipment to be used in the attack. Although implicit, this relationship between expertise and the use of equipment does not always apply—for instance, when environmental measures prevent an expert attacker's use of equipment; or when, through the efforts of others, attack tools requiring little expertise for effective use are created and freely distributed (e.g., via the Internet).

2.2.5 Access to TOE: Samples

Access to the TOE is also an important factor. It is assumed here that the TOE would be obtained by the attacker and that beside other factors there is no time limit in analysing or modifying the TOE. Differences are defined in the status and functionality of the device to be analysed/tested. This shall replace the CEM factor "Access to TOE".

- **Mechanical samples** are non-functional. Samples in this category could be the external shielding of a TOE which may be used to find out access points. These samples could be used merely to study the mechanical design, but not to study the internal HW structure or design.
- **Non-functional samples** might be used to identify the hardware structure of the TOE to detect possible tamper resistant, responding or evident countermeasures to perform the attack. TOE does not work as in the TSF (damaged TOEs, TOE sensors might be deactivated, etc.)
- **Fully functional samples** operating according to the TSF. These samples allow performing real simulations with the TOE.

Table 11: Rating for Access to TOE

Access to TOE (samples)	Identification	Exploitation
Mechanical sample	1	1
Non-functional samples	2	2
Fully functional samples	4	4

If more than one unit is required, the values must be multiplied by the factors given below.

Table 7: Factor to rate the samples

Number of Devices	Factor
1	1
2	1.5
3-4	2
5-10	4
>10	5

The Security Policy as expressed in the Security Target should also be taken into account.

2.2.6 Equipment and tools

Equipment refers to the equipment that is required to identify or exploit some vulnerability.

In order to clarify equipment category, price and availability has to be taken into account.

- **Standard equipment** is equipment that is readily available to the attacker, either for the identification of vulnerability or for an attack. This equipment can be readily obtained—e.g., at a nearby store or purchased from the Internet. The equipment might consist of simple attack scripts, personal computers, power supplies, or simple mechanical tools like standard drills, common use chemical products, soldering irons,etc.
- **Specialized equipment** is not readily available to the attacker due to its price or size, but could be acquired without undue effort. This could include purchase of moderate amounts of equipment (e.g., specialized test bench, chemical workbench, precise milling/drills, etc.) or development of more extensive attack scripts and proofs.
- **Bespoke equipment** is not readily available to the public as it might need to be specially produced (e.g., very sophisticated tools) or because the equipment is so specialized that its distribution is controlled, possibly even restricted. Alternatively, the equipment may be very expensive (e.g., Abrasive Laser Equipment). Bespoke equipment, which can be rented, might have to be treated as specialized equipment.

In an ideal world definitions need to be given in order to know what are the rules and characteristics for attributing a category to an equipment or a set of equipment. In particular, the price, the age of the equipment, the availability (publicly available, sales controlled by manufacturer with potentially several levels of control, may be hired) shall be taken into account. The tables below have been put together by a group of industry experts and **will need to be revised from time to time**.

The range of equipment at the disposal of a potential attacker is constantly improving, typically:

- Computation power increase
- Cost of tools decrease
- Availability of tools can increase
- New tools can appear, due to new technology or to new forms of attacks

It may occur that for sophisticated attacks, several types of equipment are required. In such cases by default the higher of the different equipment factors is chosen.

The border between standard, specialized and bespoke cannot be clearly defined here. The rating of the tools is just a typical example. It is a case by case decision depending on state of the art and costs involved. The following tables are just a general guideline.

Table 8: Rating for tools

Tool	Equipment
Soldering Iron	Standard
Heat guns	Standard
Glue	Standard
Needle	Standard
Syringe	Standard
Knive	Standard
Steel cutting blades	Standard
Screwdriver	Standard
Hammer	Standard
Standard drill	Standard
Drill press	Standard
Circular saw	Standard
Radial arm saw	Standard
Voltage supply	Standard

Multimeter	Standard
Analogical Oscilloscope	Standard
PC or workstation	Standard
Signal analysis software	Standard
Dental toolkit (mirrors)	Standard
Borescope	Standard
Fiberscope	Standard
Solder paste	Standard
Shunts	Standard
Wires and electrical probes	Standard
Torch	Standard
Micro-cameras	Standard
Microphones	Standard
Chemical products	Standard
Antennas	Standard
Milling Machine	Specialized
Sandblasting Machine	Specialized
CNC Milling Machine	Specialized
Laser Milling Machine	Specialized
Laser Equipment	Specialized
Electrostatic emitting devices	Specialized
Electromagnetic emitting devices	Specialized
Conductive ink printer	Specialized
Signal and function processor	Specialized
Digital Oscilloscope	Specialized
Signal/Protocol Analyser	Specialized
Tools for chemical etching (wet)	Specialized
Tools for chemical etching (plasma)	Specialized
Tools for grinding	Specialized
Climate chamber	Specialized
Anechoic chamber	Specialized
Standard X-ray machine	Specialized
Radio-frequency generator	Specialized
Gamma-ray generator	Specialized
Standard tomography scanner	Specialized
Standard thermal camera	Specialized
FIB systems	Specialized

Manufacturers know the purchasers of these tools and their location. The majority of the second hand tools market is also controlled by the manufacturers.

Efficient use of these tools requires a very long experience and can only be done by a small number of people. Nevertheless, one cannot exclude the fact that a certain type of equipment may be accessible through university laboratories or equivalent but expertise in using the equipment is quite difficult to obtain.

Table 9: Rating for tools (II)

Tool	Equipment
X-ray 3-D tomograph	Bespoke
New Tech Design Verification and Failure Analysis Tools	Bespoke

Note, that using bespoke equipment should lead to a moderate potential as a minimum.

The level “Multiple Bespoke” is introduced to allow for a situation, where different types of bespoke equipment are required for distinct steps of an attack.

Table 10: Rating for Equipment

Equipment	Identification	Exploitation
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8

(1) If clearly different testbenches consisting of specialised equipment are required for distinct steps of an attack this shall be rated as bespoke.

2.2.7 Window of Opportunity

Opportunity is also an important consideration, and has a relationship to the Elapsed Time factor. This factor applies when the identification or exploitation of some vulnerability may require considerable amounts of access to a TOE that may increase the likelihood of detection. Some attack methods may require considerable effort off-line, and only brief access to the TOE to exploit. Access may also need to be continuous, or over a number of sessions.

For the purposes of this annex:

- **Unlimited**: access means that the attack does not need any kind of opportunity to be realised because there is no risk of being detected during access to the TOE.
- **Easy**: means that access is required for less than an hour.
- **Moderate**: means that access is required for less than a day.
- **Difficult**: means that access is required for at least a week or more.
- **None**: means that the opportunity window is not sufficient to perform the attack (the length for which the asset to be exploited is available or is sensitive is less than the opportunity length needed to perform the attack - for example, if the asset key is changed each week and the attack needs two weeks).

Consideration of this factor may result in determining that it is not possible to complete the exploit, due to requirements for time availability that are greater than the opportunity time.

Table 11: Rating for the Windows of Opportunity

Window of opportunity	Identification	Exploitation
Unlimited	0	0
Easy	1	1
Moderate	2	3
Difficult	4	5
None	-*	-*

* Indicates that the attack path is not exploitable due to other measures in the intended operational environment of the TOE

2.2.8 Final table

Table 12: Final table for the rating factors

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
≤ one day	1	2
≤ one week	2	3
≤ one month	3	4
> one month	5	7
Expertise		
Layman	0	0
Proficient	1	1
Expert	2	3
Multiple Expert	5	6
Knowledge		
Public	0	0
Restricted	2	2
Sensitive	3	4
Access to TOE (Samples)		
Mechanical sample*	1	1
Functional samples without working keys*	2	2
Functional samples without working keys*	4	4
Equipment		
None	0	0
Standard	1	2
Specialized**	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Window of opportunity		
Unlimited	0	0
Easy	1	1
Moderate	2	3
Difficult	4	5
None	-***	-***

* Table 7 contains an factor to rate the number of devices.

** If clearly different test benches consisting of specialised equipment are required for distinct steps of an attack this shall be rated as bespoke.

*** Indicates that the attack path is not exploitable due to other measures in the intended operational environment of the TOE.

2.2.9 Range

The following table replaces table 4 of section B.4 of CEM for the domain “Hardware Devices with Security Boxes”.

Table 13: Rating of vulnerabilities

Range of Values*	TOE resistant to attackers with attack potential of
0 – 13.5	No rating
14– 15.5	Basic
16 – 24.5	Enhanced – Basic
25 – 34.5	Moderate
35 and above	High

* Final attack potential = identification + exploitation

3 APPLICATION OF ATTACK POTENTIAL

The attack potential rating is performed following the strategy presented in **Section 2 Parameters conditioning attacks**. The calculation of the attack potential will be performed by adding the ratings of two phases: identification and exploitation.

For every attack described in the following sections, special annotation, called **Rating hint**, has been added. This note consists in several hints which may help the evaluator to determine the proper attack potential rating to be calculated, taking into account the different scenarios that the attacker will face.

3.1 Physical security invasive attacks

3.1.1 Attacks to external Enclosures

3.1.1.1 Manual Material Removal Attacks

The following attacks bypass any external enclosure in order to disclose critical design information or secret data (data travelling through any bus):

- De-attach tamper evident stickers: open a security box, sealed with tamper evidence stickers, leaving no tamper evidence e.g. applying hot air on a sticker until it gets sticky, and then just carefully remove it.
- Bypass tamper screws: the special-head screws can be sometimes removed by mechanical procedures e.g. drilling the head of the screw and then remove the screw with pliers.
- Remove (glued) covers: heat can make the glue become malleable e.g. heating the glue with a hairdryer will make it sticky and easy to remove.
- Brain surgery: the attacker attempts to remove material, in a lot amount of time and very carefully, from a potted or sealed container while stopping short of tripping a sensor e.g. using a knife or any other accurate cutting tool.

Rating hint: take into account that depending on the type of seals used to leave tamper evidence, the attacker can remove the stickers from easy by using only a hairdryer to difficult process trying to leave no evidence when a really specialized tamper evident sticker is used. In addition, the brain surgery attack must not be underestimated, if the attacker has good hand-eye coordination and is plenty of time, extremely delicate work can be accomplished.

The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.1.2 Mechanical Machining Attacks

The following attacks bypass any external enclosure in order to disclose critical design information or secret data (data travelling through any bus):

- Automatic material removing: remove potting material in an automatic way e.g. milling out the epoxy resin to discover any underneath device.

Rating hint: the mechanical machining process, from dummy tools to computer numerical control (CNC) machines, extremely depends on the scale factor of the security box. A research may allow the evaluator to assess the required precision for the attack so that he can determine which kind of machine is needed and how much time it takes .

The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.1.3 Water Machining Attacks

The following attacks bypass any external enclosure in order to disclose critical design information or secret data (data travelling through any bus):

- Water machining: remove potting material using a water jet cutter e.g. removing the epoxy material layer by layer.

Rating hint: the water jet cutter process extremely depends on the scale factor of the security box. A research may allow the evaluator to assess the required precision for the attack so that he can determine which kind of machine is needed and how much time it takes.

The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.1.4 Laser Machining Attacks

The following attacks bypass any external enclosure in order to disclose critical design information or secret data (data travelling through any bus):

- Laser machining: remove potting material using a Laser cutter e.g. removing the epoxy material layer by layer.

Rating hint: the Laser cutting process extremely depends on the scale factor of the security box. A research may allow the evaluator to assess the required precision for the attack so that he can determine which kind of machine is needed and how much time it takes.

The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.1.5 Sandblasting Attacks

The following attacks bypass any external enclosure in order to disclose critical design information or secret data (data travelling through any bus):

- Sandblasting machining: remove potting material using sandblasting machining e.g. removing the epoxy material layer by layer.

Rating hint: the sandblasting machining process extremely depends on the scale factor of the security box. A research may allow the evaluator to assess the required precision for the attack so that he can determine which kind of machine is needed and how much time it takes.

The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.2 Switches deactivation attacks

3.1.3 Sensors removal and deactivation

The following attacks bypass any sensor in order to disclose critical design information or secret data (data travelling through any bus):

- Bypass the sensor: those sensors based in all-or-nothing detection, can by bypassed depending on its constructive nature e.g. soldering the pads, between them, of a micro switch detector.
- Remove the sensor: the sensor can be mechanically removed from its position e.g. carefully hammering the sensor with a pry tool.
- Deactivate the sensor: the sensor can be disconnected from its measuring source e.g. covering an ambient light sensor with black epoxy.

Rating hint: the evaluator may take into account the specific topology of the sensors. The scale factor must be considered as a critical factor in the calculation of the attack potential. When the attacker is facing any macroscale sensor, the attack methodology is going to be less time consuming then other types. Since the integration of IC is becoming extremely common, the attacker will face in many cases sensor sizes around the nanometers.

The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.4 Attack to a tamper respondent sensor networks

The following attacks bypass any sensor network in order to disclose critical design information or secret data (data travelling through any bus):

- Sniff the network: the sensor network can be monitored using an external device such as bus readers/analyzers e.g. if the sensor is externally accessible, it can be monitored using any bus reader.
- Modify the sensor behaviour: the sensor can be modified by adding a fixed value to its data register e.g. the data register can be access using any JTAG which may allow the attacker to fix the measured value.

Rating hint: the evaluator has to take into account that some of the implementation can be easier to sniff than others. If the bus (I2C, SPI, RS232, ...) is encrypted, the effort will be extremely higher compare to those buses in plaintext.

The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.5 Removing and penetration potting materials

The following attacks bypass any enclosure based in epoxy materials in order to disclose critical design information or secret data (data travelling through any bus):

- Solve the epoxy material: the epoxy resin can be removed by using chemical products e.g. injecting the proper chemical solvent over the epoxy material.
- Remove the epoxy material mechanically: the epoxy resin can be removed mechanically, removing layer by layer e.g. carefully hammering the epoxy with a pry tool.

Rating hint: The more time spent studying the epoxy formulae the more efficient solvent will be found for the chemical removing process. In addition, sometimes a tamper mesh, usually a very long loop of wire, is embedded in the epoxy. If the wire material is similar to the epoxy chemical formulae, the solvent applied will destroy the tamper detection wire at the same time, causing a high risk of tamper detection or destruction of the internals.

The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.6 Penetration of tamper respondent meshes

The following attacks bypass any tamper response mesh in order to disclose critical design information or secret data (data travelling through any bus):

- Open a hole by adding and cutting pieces of the conductive tracks: bypassing some of the conductive tracks of the mesh may allow drilling a hole directly on the mesh e.g. by inserting a needle in between two tracks.
- Short-circuit the connector of the mesh: if the tracks to the connector between the mesh and the PCB are reachable, the conductive tracks can be short-circuited adding any conductive material e.g. soldering the connector pads between each other.

Rating hint: The time spent studying the track layout inside the mesh will allow the attacker to increase the opportunity of success when inserting a needle or similar. On the other hand, some tamper respondent meshes may contain conductive tracks with a very similar composition to the isolating layers at the mesh. This issue may increase the risk of tampering detection in case of mechanical removal or penetration of the mesh.

The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.7 Direct attack to the Anti-tamper processor

The following attacks bypass any anti-tamper processor in order to disclose critical design information or secret data (data travelling through any bus):

- Shaped charge shooting: extremely high precision shooting of shaped charges can penetrate a package causing its circuits to be disabled before they can respond e.g. a memory zeroing circuit can be disabled before the energy can be removed from the memory.
- Energy attacks: by focusing a high energy beam on the processor its functionality can be modified or stopped e.g. shooting an electromagnetic pulse focused on the anti-tamper processor.

Rating hint: In this kind of attacks, another attack path may be considered. Since it is necessary to determine the exactly location of the processor inside the PCB, tomography or X-ray technologies may apply. On the other hand, some cases may include anti reverse engineering methods, 3D mapping or X-ray imaging protection. This issue can be solved by probing the internals of the box through a slit or hole which belong to the design or maybe has been manually created bypassing other kind of tamper detections. Notice, the attack will increase its potential rating since other protections may be active e.g. light detectors on the top of the PCB may detect the light coming from a small hole.

The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.8 Direct attack to the auxiliary battery

The following attacks bypass any anti-tamper processor, which depends on an external power supply, in order to disclose critical design information or secret data (plaintext buses):

- Deactivating the auxiliary power supply: interrupting the power supply which maintains the security processor running when the external power supply is gone e.g. cutting the wire or track of the auxiliary external battery supply.
- Extremely power consumption: by focusing a high energy beam on the auxiliary battery location e.g. shooting an electromagnetic pulse focused on the auxiliary battery.

Rating hint: In this kind of attacks, another attack path may be considered. Since it is necessary to determine the exactly location of the battery inside the PCB, tomography or X-ray technologies may apply. On the other hand, many cases may include an external auxiliary battery; in such cases cutting the power supply becomes extremely easy. However, the attacker may consider that the elapsed time between the action of cutting the wire and the zeroization of the memory can be extremely short.

The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.2 Physical security semi-invasive attacks

3.2.1 Perturbation attacks

The following attacks bypass any anti-tamper processor, which depends on an external power supply, in order to disclose critical design information or secret data (data travelling through any bus):

- Permanent environment perturbations: an attacker may need to change the environment conditions during the whole time that the attack is performed e.g. increase/decrease the temperature of the execution environment until the maximum/minimum allowed temperature is reached trying to obtain information from a RAM module.
- Transient perturbations: by changing the environment condition values in short times of the running period e.g. increasing the voltage in the power supply suddenly, anomalies can be detected in the behaviour of a system.

Rating hint: In this kind of attacks, the evaluator may consider the knowledge of the system required to perform such perturbations. For example, if the system has a temperature sensor fixed to certain value, the effort of getting the value must be considered in terms of: available source code (open source), reverse engineering methods, ...

The main impacts are:

- Disclosure of any critical security information.

3.3 Physical security non-invasive attacks

3.3.1 Reverse engineering

3.3.1.1 Imaging technologies

The following attacks bypass any anti-reverse engineering system in order to disclose critical design information or secret data (plaintext stored data):

- Visual / Optical recognition: Probably all the reverse engineering methodologies begin with this step, the attacker will try to recognise the structure of the security box by visual recognition e.g. having a look through a hole with the help of a torch.
- X-ray snapshot: The x-ray recognition will help the attacker guessing the structure of the internals protected by the box e.g. taking an x-ray of the security box will sometimes reveal the internals design.
- Ultrasound Attacks: Ultrasound imaging is carried out by means of sound waves with frequency beyond the range of 20,000 Hz. This technique is useful to see wires, hardware components, chemical protections, etc. and to detect breaches and gaps in surfaces.
- Tomography Attacks: Taking a tomogram of a system, the attacker can obtain very critical information about the different levels of the internal design of a system e.g. the attacker will take a tomogram of a multi-layer PCB, this will allow the attacker guessing the internals of the PCB.
- Thermography Attacks: During execution time, the attacker will take a thermal image which can be used to guess the internal structure e.g. the attacker will take the thermal image trying to obtain the disposition of the main ICs.

Rating hint: For every method described above, the evaluator has to take into account the measures taken in the design of the system. Some anti-reverse engineering protection mechanisms will obfuscate the components layout increasing severely the identification of the ICs used in the implementation. On the other hand, if the system is protected against x-ray, tomography or any other kind of 2D/3D scanning methodology, the evaluator has also to take into account the necessary effort to be apply in case of bypassing or deactivating such mechanisms.

The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of the stored plaintext data.

3.3.2 Power consumption analysis

The following attack has been designed to try to disclose critical secret data (key ciphered data):

- Power consumption analysis: power consumption measurements are collected, from the power supply line, during cryptographic operations e.g. the attacker will insert any small resistor in series with the power input, then the voltage difference across the resistor divided by the resistance value yields the current value.

Rating hint: the evaluator may consider that this kind of analysis is highly difficult. The number of samples to be taken and the study to be implemented after taking the measurements is based in complex differential analysis. The evaluator should consider the expertise required to the attacker in order to get some valuable information such as the key used in the calculations.

On the other hand, as the security box protects properly the accessibility to the internals, the power consumption analysis shall be performed using a TOE external interface.

The main impacts are:

- Disclosure of the stored ciphered data.
- Disclosure of the secret keys.

3.3.3 Emanation analysis

The following attack has been designed to try to disclose critical secret data (secret keys or ciphered data):

- Emanation analysis: an antenna sited close to the chip will read the electromagnetic field variations induced in the surrounding area of the device e.g. the attacker will attach an antenna close to the IC and analyze the wave form depicted in the oscilloscope during a time.

Rating hint: the evaluator may consider that this kind of analysis is highly difficult. The number of samples to be taken and the study to be implemented after taking the measurements is based in complex differential analysis. The evaluator should consider the expertise required to the attacker in order to get some valuable information such as the key used in the calculations.

On the other hand, as the security box protects properly the accessibility to the internals, the emanation analysis shall be performed locating an antenna outside the security box boundary.

The main impacts are:

- Disclosure of the secret keys.

3.3.4 Timing analysis

The following attack has been designed to try to disclose critical secret data (secret keys or ciphered data):

- Execution time analysis: an analysis of the variations of execution time of an operation in a cryptographic algorithm, which may reveal knowledge of or about a critical security parameter such as a PIN or cryptographic key e.g. the attacker will execute different cryptographic functions while measuring the spent time.

Rating hint: usually this kind of analysis can be performed by using the external interfaces of the system. However, if the cryptographic timing is not reacheable from the outside, an extra effort must be taking into account, for example trying to determine the time consumed by an internal cryptographic library performing calculations.

The main impacts are:

- Disclosure of critical security information.

APPENDIX A: HARDWARE SECURITY MODULE (HSM)

A.1 Overview

This appendix defines the attack potential rating to be applied against HSMs.

A.2 Electromagnetic and sounds analysis

The following attack has been designed to try to disclose critical secret data (secret keys or ciphered data):

- PIN-pad entry: the secret PIN number can be guess during the code entering procedure e.g. the attacker will attach a small microphone close to the PIN-pad, will record the sound of the hit keys and later on guess the secret number.
- Emanation analysis: an antenna sited close to the chip will read the electromagnetic field variations induced in the surrounding area of the device e.g. the attacker will attach an antenna close to the IC and analyze the wave form depicted in the oscilloscope during a time.

Rating hint: the evaluator may consider the effort when trying to hide any electrical device in case of recording sounds. For example, is might be easy to hide a nano-microphone in the PIN-pad. Hints regarding the emanation analysis are given in section 3.3.3 of this annex.

The main impacts are:

- Disclosure of the secret keys.

APPENDIX B: TACHOGRAPH

B.1 Overview

This appendix defines the attack potential rating to be applied against Tachographs.

B.2 PIN-based (keyboard) authentication

B.2.1 Electromagnetic and sounds analysis

The following attack has been designed to try to disclose critical secret data (secret keys or ciphered data):

- PIN-pad entry: the secret PIN number can be guessed during the code entering procedure e.g. the attacker will attach a small microphone close to the PIN-pad, will record the sound of the hit keys and later on guess the secret number.
- Emanation analysis: an antenna sited close to the chip will read the electromagnetic field variations induced in the surrounding area of the device e.g. the attacker will attach an antenna close to the IC and analyze the wave form depicted in the oscilloscope during a time.

Rating hint: the evaluator may consider the effort when trying to hide any electrical device in case of recording sounds. For example, is easier hiding a nano-microphone in the PIN-pad. Hints regarding the emanation analysis are given in section 3.3.3 of this annex.

The main impacts are:

- Disclosure of the secret keys.

B.2.2 Printer drawer

The following attack has been designed to try to disclose critical design data:

- Printing paper replacement: For those tachographs including a printing device, paper replacement becomes a challenge. In many situations, the drawer containing the replaceable paper leaves a big opening. An attacker can insert almost any tool through this hole making the internals of the printer reachable e.g., the attacker will probe the internals of the tachograph using a fiberscope camera through the printing drawer hole.

Rating hint: the evaluator may consider if the opening left by the printer drawer is easily reachable or not. If the drawer opening is filled with black epoxy, other machining methods must be used, therefore additional rating must be considered.

The main impacts are:

- Disclosure of secret design information.

36. ANNEX 10: MINIMUM ITSEF REQUIREMENTS FOR SECURITY EVALUATIONS OF HARDWARE DEVICES WITH SECURITY BOXES

PURPOSE

This annex provides requirements related to the minimum capabilities an accredited ITSEF shall have in its premises to conduct the different types of attacks present in Annex 9, APPLICATION OF ATTACK POTENTIAL TO HARDWARE DEVICES WITH SECURITY BOXES. These capabilities include the knowledge and the skills of their evaluators and the necessary equipment, and evaluation methodology description, all necessary to conduct the attacks mentioned above.

PARTICULAR STATUS

None.

CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE

Chapter 6, SPECIFIC REQUIREMENTS APPLICABLE TO A CAB
Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS.

1 REQUIRED CAPABILITIES FOR THE PHYSICAL EVALUATION OF HARDWARE DEVICES WITH SECURITY BOXES

1.1 Overview of a Physical Evaluation

The physical evaluation of hardware devices with security boxes (HDwSB) requires the development of specific skills and knowledge. The aim is to provide a technical guidance for evaluators running an evaluation and to expose the related minimum requirements.

To achieve this, the following sections will encompass:

- The understanding of the secure physical technology, its underlying principles and the development equipment used by manufacturers.
- The knowledge and experience in physical attack techniques that could compromise the hardware and an ability to use the related equipment to stress the hardware layers. This includes the understanding of the underlying physical principles.
- The ability to use the related equipment to conduct physical disruptions and the understanding of the related physical effects on the hardware.
- The knowledge and experience in cryptographic attack techniques and the ability to perform the analysis (including data-capture, signal processing procedures, analysis and rating).

The required tools for performing the various attack techniques can be categorised in standard (basic), specialised and bespoke.

1.2 Physical Technology

Evaluators must understand typical HDwSB hardware and the underlying principles to the extent necessary to comprehend the design decisions of the manufacturer.

Basic knowledge of the following is required:

- the electrical behaviour of electronic components, e.g. resistors, capacitors, transistors, integrated circuits, RAM, ROM, E2PROM, etc,
- design principles of integrated circuits,
- chemical properties of typical HDwSB hardware.

In addition, evaluators must have detailed knowledge of:

- microcontroller architecture, functionality and packaging,
- architecture and functionality of FPGAs (Field Programmable Gate Array) and ASICs (Application Specific Integrated Circuit),
- physical behaviour of removal and case opening detection switches,
- physical behaviour of sensors (temperature, voltage, …),
- layout principles of PCBs (Printed Circuit Boards),
- physical principles of protective shields (e.g. grid foils, printed grids),
- realisation of standard circuitry as used in micro-controllers,
- dynamic behaviour of digital and analogue circuitry,
- physical behaviour of potting mechanisms.

Evaluators must be able to understand the schematics (block diagrams, schematics).

Evaluators must have knowledge of the design process and must understand the process from the schematics (logical representation of the hardware) to the actual layout (physical representation). They must understand the processes of technology qualification, functional testing, characterisation, and reliability testing.

Evaluators must understand the development equipment used by the manufacturers for micro-controller software. This includes simulators, emulators, and special evaluation software tools. They must be able to read micro-controller source code and to develop software for penetration testing and other investigations. Therefore, evaluators must understand the CPU instruction set, the memory map and use of other peripheral units of the micro-controller.

1.3 Physical Specific Attacks

The following provides an overview about HDwSB specific attacks. This is not a complete list but provides some examples. Detailed information about HDwSB specific attacks can be found in Annex 9, APPLICATION OF ATTACK POTENTIAL TO HARDWARE DEVICES WITH SECURITY BOXES.

Evaluators must have knowledge about standard attack scenarios and in principle be able to develop new ideas for such attacks.

To be more specific, evaluators must know about attack scenarios for HDwSB such as intrusion of sensors, switches and filters, physical manipulation and probing, malfunction attacks, inherent and forced leakage attacks, abuse of test features and cryptographic attacks. A multitude of such attack scenarios – along with quotations – is described in the Annex cited above.

Evaluators shall be able to adapt and combine these attack scenarios for the individual HDwSB being subject to evaluation. During vulnerability analysis they must be able to find possible weaknesses (in schematics and their realisation on the HDwSB and the combination thereof) and be able to use the standard techniques to assess them.

Evaluators must have knowledge and experience of other HDwSB attacks; side channel attacks (SCA) such as Timing Analysis, Machine Learning based SCA, Simple Power Analysis (SPA), Differential Power Analysis (DPA), Differential EM radiation Analysis (DEMA), Template Attacks (TA); fault injection attacks such as DFA and related attacks) and possess the equipment (physical and analysis tools) necessary to perform such attacks. The ITSEF must own or have unlimited access to the equipment (physical and analysis tools) necessary to perform such attacks according to section 1.4. They must be able to operate this equipment (including data-capture procedures) and to perform the analysis (mathematics). Knowledge and experience in cryptography and standard cryptographic attack techniques is required.

Evaluators must at least understand the physical principles, and the usage (as appropriate) of the equipment classed as 'standard', 'specialised' and 'bespoke' as defined in Annex 7, APPLICATION OF ATTACK POTENTIAL TO SMARTCARDS AND SIMILAR DEVICES.

1.4 Equipment for HDwSB Physical Evaluation

In order to accomplish the vulnerability and failure analysis, physical manipulations and attack scenarios mentioned in section 1.3, the ITSEF must have unlimited access to and own the majority of the tools of the category 'standard' and shall be able to use them efficiently.

The ITSEF must have unlimited access to tools of the category 'specialized' and shall know how to use them efficiently.

Examples of this equipment and their categorisation are listed in Annex 9, APPLICATION OF ATTACK POTENTIAL TO HARDWARE DEVICES WITH SECURITY BOXES.

The ITSEF must at least possess a basic set of tools (unlimited access is not sufficient) for physical manipulations, side channel analysis, perturbation attacks and supply equipment. The supply equipment is needed for the operation of the TOE during the evaluation.

The basic set consists of the following tools:

- soldering iron, solder paste, heat guns, glue, needles, syringes, knives, steel cutting blades, screwdriver, hammer, standard drill, saws, dental toolkit (mirrors), tools for chemical etching, tools for grinding,
- multimeter, digital oscilloscope, signal/protocol analyser, PC or workstation, signal analysis software, shunts, wires and electrical probes, digital camera, endoscope, microphones, electric torch, antennas,
- voltage supply devices, signal and function generators.

2 REQUIRED CAPABILITIES FOR A LOGICAL HDWSB EVALUATION

2.1 HDwSB Logical Design

Evaluators must understand typical HDwSB logical architectures (e.g. the boot process, operating system, resource management and interfaces) and the underlying principles to the extent necessary to comprehend the design decisions of the HDwSB developer. They must know the typical potential HWSB vulnerabilities and standard test and attack methods, especially domain-specific attack methods.

Evaluators must show their ability to search for new publicly known vulnerabilities.

2.1.1 Source Code

A typical HDwSB runs software on dedicated hardware. Therefore, knowledge of software, how it is designed, compiled and executed and how it utilizes the hardware is important for the evaluation.

A wide array of programming languages can be used to write the software found in a HWSB. They can be categorized into three families:

- Low level: specific to the processor of the HWSB language (ARM assembler, x86 assembler, etc.),
- Intermediate level: compiled code (C, C++, ADA, GO, Rust etc.),
- High level: managed code, running inside a virtual machine or an interpreter (Java, Python, Shell, Perl, PHP etc.).

Now while assembler is less used, managed code, on the opposite, can often be encountered, as well as compiled code. Evaluators need a thorough understanding of the use of C/C++ or Java in the context of the specific hardware architecture. If the HDwSB in evaluation or parts of it are programmed in other languages evaluators need a thorough understanding of these languages, too.

Moreover, for an in-depth security analysis, an understanding of assembler code and intermediate code (like Java Card byte code) is required. In particular, a variety of security impacts and defects cannot be understood on the level of a higher language like C or Java, because they become only apparent in assembler code or byte code. Therefore, the importance of understanding assembler code produced by a compiler and security impacts of generation tools shall be explicitly emphasized – eventually the processor runs on assembler (machine) code, not C, Java or anything else.

In addition, evaluators need to understand the impact of compilers, compiler libraries and interpreters on the security behaviour of the HDwSBs in evaluation. They must know the meaning of the different compiler settings in relation to security aspects (e.g. if an optimization flag removes loops necessary to avoid timing attacks).

2.1.2 Interfaces

Evaluators shall be familiar with the different kind of interfaces which are typically used by HDwSBs, e.g. Universal Serial Bus (USB), Serial, Ethernet port, Near Field Communication (NFC), Wi-Fi and Bluetooth. If a HDwSB uses other kinds of interfaces they shall be familiar with them, too.

They must know if the interfaces allow potentially security-critical behaviour, e.g. direct memory access (DMA) or modes of operations which are not foreseen by the developer. Evaluators must know how to address the HDwSB interfaces at the different ISO OSI layers and how to test their correct function.

They shall also be able, through software, to utilize debug ports available on the PCB, such as JTAG.

Evaluators must have knowledge of penetration tests related to the above mentioned interfaces.

2.1.3 Transport Layer Protocols

Evaluators must have knowledge of the security principles of the encryption schemes to be used for the transport layer protocols like secure messaging at smart card interfaces or TLS or SSH over the interfaces detailed in the above section.

Often these standards allow a high degree of flexibility in the configuration of security options, demanding scrutiny when evaluating a specific choice against a set of prerequisite requirements.

Evaluators must have knowledge of penetration tests related to the above mentioned transport layer protocols.

2.1.4 Application Layer Protocols

Evaluators must have knowledge of the security behaviour of application layer protocols, e.g. for POI knowledge of payment protocols like EPAS, IFSF (online) and EMV. Further examples are the processing of GNSS data in digital tachograph environment and the usage of the PACE protocol in smart meter gateways. They must know the security related state machines of these protocols as well as the underlying cryptographic mechanisms. They must be able to use test suites implementing such protocols to test security features of these protocols.

Evaluators must have knowledge of the typical PIN encryption schemes.

They must know the security principles of key management, HDwSB management protocols and software download mechanisms.

2.1.5 Operating System, Content and Resource Management

The defining task of an operating system is the management of computational resources (like persistent and volatile memory, internal I/O, external interface components, display, keyboard, etc.) and the administration of access (interface) to such resources.

While the previous paragraphs dealt with the communication between a HDwSB and the outside world, the focus shall lie here on the resource management inside the HDwSB itself.

At first, evaluators need to understand the different types of operating systems and their specifics, e.g. a real-time OS will not behave the same way as a standard desktop OS. Also the file structure and file access rights administration within these various operating systems will differ. Knowledge of the memory types (EE, Flash, ROM, RAM), special dedicated RAM (like Crypto-RAM, Buffer-RAM) and memory management procedures (e.g. access limitations) are required.

The concept of domain separation and application isolation needs to be profoundly understood. This is especially relevant for application management, which refers to the secure loading, administration, deletion of application as well as the access rights of such applications to the HDwSB's resources. This concept of separation is typically assisted by the underlying hardware/firmware platform, such as with the Trusted Execution Environment (TEE). It is important for the evaluator to have knowledge in this specific area.

The concept of boot-up processes for embedded devices, e.g. of multi-stage bootloaders, and the various possibilities of updating firmware and operating systems needs to be profoundly understood. Boot-up and update processes are potential targets for an attacker.

Another potential attack path might be the error handling e.g. in case of unexpected or misaligned expression as input. The evaluator must be able to analyse the error handling and to conduct appropriate tests.

2.1.6 Random Number Generator

The evaluator must have knowledge of and experience with evaluation methodologies for random number generators, in particular according to ISO/IEC 20543[65].

For the evaluation of physical RNGs the evaluator must have sufficient knowledge in probability theory and design principles of physical RNGs. The evaluator must be able to identify and analyse those characteristics of a system or a process that have significant impact on the distribution of random numbers and to rate the randomness of number generation.

This analysis shall be quantified by a stochastic model. The stochastic model shall allow to verify a lower entropy bound per random bit. The stochastic model in particular comprises a family of distributions that contains the true (but unknown) distribution(s) of the raw random numbers (or at least of random numbers in an early stage of the generation process) during the life time of a physical RNG, even for defective states, e.g. unacceptable outputs. The stochastic model shall be justified by technical arguments. Furthermore, also the effectivity of online tests (also known as "health tests") shall be verified on the basis of the stochastic model.

2.2 Equipment for HDwSB Logical Evaluation

In order to accomplish the vulnerability and failure analysis and attack scenarios mentioned in section 1.3, the ITSEF must have unrestricted access to the following categories of tools necessary to perform those analysis and attacks:

- Environment control equipment (e.g. to control communication, voltage, clock and temperature);
- Chemical and mechanical lab equipment (i.e. for sample preparation and analysis);
- Imaging equipment (e.g. cameras, microscopes);
- Logical test tools (e.g. for interface testing, vulnerability scanning, operating system testing, randomness analysis, source code analysis, circuit layout analysis, fuzzing tools).

Evaluators shall be able to operate the equipment to perform independent tests and attacks.

3 ITSEF ORGANISATION

3.1 Life cycle

Evaluators have to know the main phases of the life cycle which are the following: Development and manufacturing, initial software loading, delivery, installation and operation (including loading of software updates and additional software),and end-of-life (e.g. controlled erasure of keys and destruction or re-use of hardware).

3.2 Subcontracting, third party facilities and equipment

General conditions for subcontracting and for the use third party facilities and equipment are defined in Chapter 7, NOTIFICATION AND AUTHORISATION OF CABS, FUNCTIONING OF CABS AND SUBCONTRACTORS.

Some attack methods for HDwSB may require specific chip know how and bespoke chip equipment. In that case this kind of work can be subcontracted to an ITSEF competent for the Technical Domain related to smartcards and similar devices.

4 ACRONYMS

EMV	Europay, MasterCard and Visa
EPAS	Electronic Protocols Application Software
HDwSB	Hardware Device with Security Box
IFSF	International Forecourt Standards Forum
OSI	Open Systems Interconnection
PIN	Personal Identification Number
SSH	Secure Shell
TLS	Transport Layer Security

[65] ISO / IEC 20543:2019: Information Security - Security Techniques - Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408.

37. ANNEX 11: ASSURANCE CONTINUITY

PURPOSE

This annex defines minimal requirements for Assurance Continuity associated with the maintenance of certificates.

PARTICULAR STATUS

None.

CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE

Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES
Chapter 14, VULNERABILTY HANDLING

1 INTRODUCTION

This annex defines minimal requirements for Assurance Continuity and associated to the maintenance activities related to:

-the reassessement that an unchanged certied ICT product still meets its security requirements;
-the evalution of the impacts of changes to a certified ICT product on its certificate.

This annex covers the following aspects of Assurance Continuity:

- Description of technical concepts underpinning the assurance continuity paradigm including a description of the processes involved in the previously described maintenance activities.
- Criteria for the characterisation of changes.
- Guidance on performing impact analysis.
- Requirements for content and presentation of an impact analysis report.

2 TECHNICAL CONCEPTS

2.1 Assurance Continuity Purpose

The purpose of Assurance Continuity is to enable developers to support the maintenance activities related to ICT certified products, as defined in Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES, and where applicable, to vulnerability handling, as defined in Chapter 14, VULNERABILTY HANDLING.

The awarding of a Common Criteria evaluation certificate signifies that all necessary evaluation work has been performed to convince the certification body that the TOE meets all the defined assurance requirements as grounds for confidence that an ICT product or system meets its security objectives.

Assurance Continuity support the activities as to maintain confidence in a certified product which certificate is soon to expire or that has submitted to changes of its TOE or its environment, and allows that evaluation work previously performed need not be repeated in all circumstances. Assurance Continuity therefore defines an approach to minimising redundancy in ICT Security evaluation, allowing a determination to be made as to whether independent evaluator actions need to be re-performed.

2.2 Terminology

For clarity, the following terms are used in this description.

The certified TOE refers to the version of the TOE that has been evaluated and for which a certificate has been issued.

The changed TOE refers to a version that differs in some respect from the certified TOE; this could be, for example:

- a new release of the TOE or of the product in which the TOE is a subset of functionality.
- the certified TOE with patches applied to correct discovered bugs.
- the same basic version of the certified TOE, but in a new operational environment (e.g. on a different hardware or software platform) as reflected in a new Security Target.

The changed TOE refers to a modified TOE that has undergone the maintenance process and to which the terms of the certificate for the initially certified TOE also applies. This signifies that assurance gained in the certified TOE also applies to the maintained TOE.

The re-assessed TOE refers to a previously certified TOE that has undergone a re-assessment.

The certificate maintenance addendum refers to a notation, such as on the listing of evaluated products, that serves as an addendum added to the certificate for a certified TOE. The maintenance addendum lists the changed versions of the TOE, that may be provided in a updated version of the certificate.

The Impact Analysis Report (IAR) refers to a report which records the analysis of the impact of changes to the certified TOE. The IAR is generated by the developer who is requesting a maintenance of the certified ICT product.

The maintenance report refers to a publicly available report that describes the changes made to the certified TOE and the results of activities necessary to the certification of the changed product.

The assurance baseline refers to the culmination of activities performed by both the evaluator and developer resulting in a certified TOE, recorded or submitted as evidence and measurable by change to that evidence.

The developer evidence refers to all items made available to the evaluators in support of an evaluation of a TOE.

A maintained certificate refers to the process of recognising that a set of one or more changes made to a certified TOE (or to aspects of the development environment) have not adversely affected assurance in that TOE, which corresponds to a re-issued (new) certificate for the changed TOE.

Re-evaluation refers to the process of recognising that changes made to a certified TOE (or to other assurance measures) require independent evaluator activities to be performed in order to establish a new assurance baseline. Re-evaluation seeks to reuse results from a previous evaluation. The positive result of a re-evaluation should lead to a new certificate with, where applicable, an extended validity period as compared to the original one.

Re-assessment refers to the process of updating the vulnerability analysis of the initially certified product, at the same level as initially requested within the security target, including when necessary the associated penetration tests. Re-assessment can be peformed ad hoc or on a periodical basis. It can be seen as a particular case of re-evaluation where the TOE has not changed, but where the changes in the threat environment need to be assessed to confirm the TOE still reaches the same level of resistance as initially certified. The positive result of a re-assessment leads to the renewal of the certificate with an extended validity period as compared to the original one.

The development environment addresses all procedures relating to development, delivery, start-up and flaw remediation of the TOE. It includes all concepts covered by the ALC class, together with the AGD_PRE family.

A subset evaluation is applicable where minor changes to the TOE include changes to the development environment. A ITSEF identifies those assurance components that are impacted by the changes to the development environment, and re-evaluates only those assurance components in light of the changes, producing a partial ETR.

A partial ETR is an output from the subset evaluation. It is created by the evaluation facility that performed the subset evaluation and provides, for the impacted assurance components, a level of detail that is commensurate with the corresponding sections of the ETR for the original certified TOE.

2.3 Assurance continuity paradigm

Assurance continuity seeks to exploit the fact that as changes are made to a certified TOE or its environment, evaluation work previously performed need not be repeated in all circumstances. The assurance continuity paradigm therefore defines the processes for certificate maintenancethrough re-evaluation and re-assessment such that each seeks to recognise previous evaluation work.

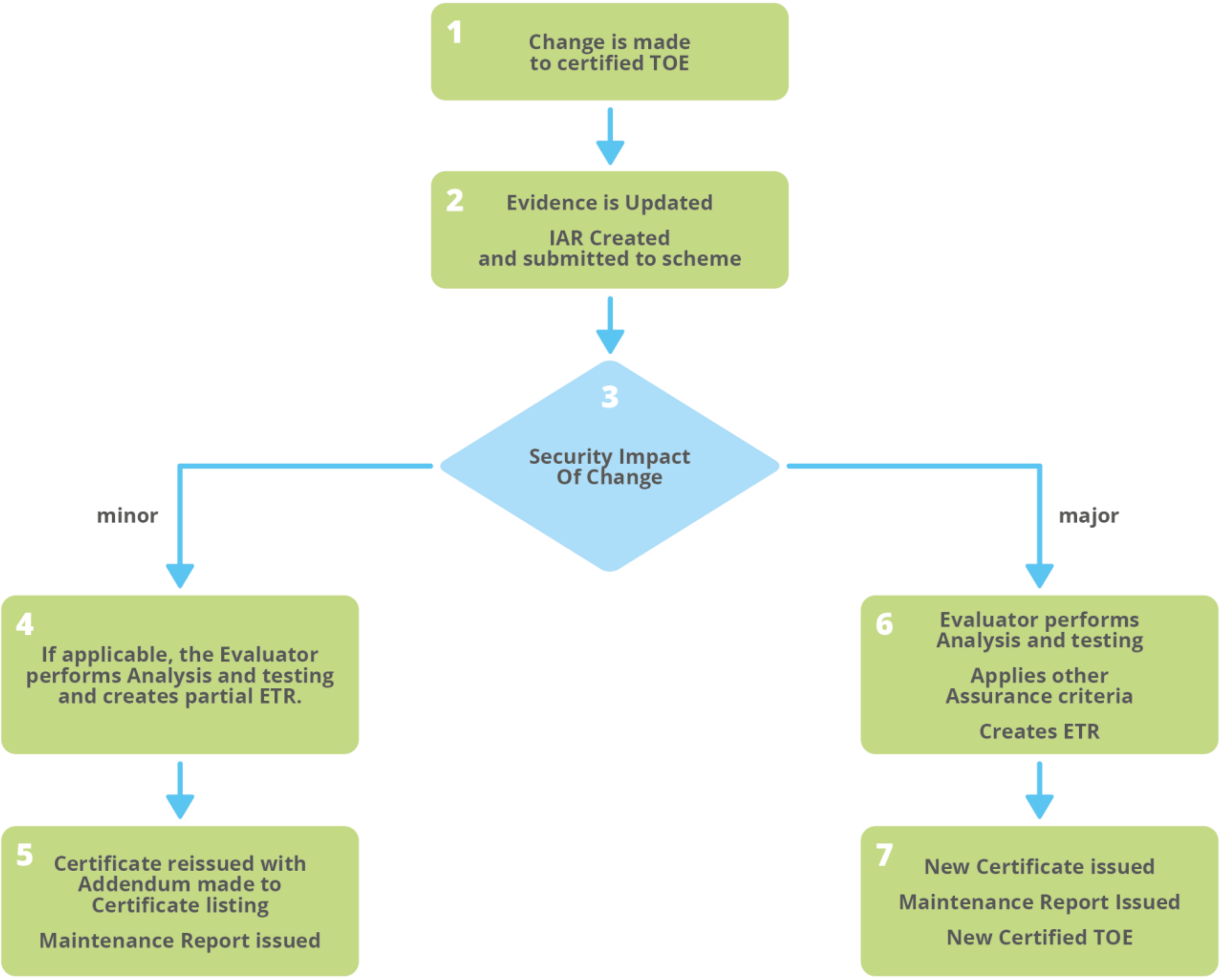
Certificate maintenance activities refer to the process undertaken by a developer in order to have a TOE, listed in the maintenance addendum for that TOE. It must be demonstrated that the changes to the TOE, the IT environment and/or the development environment do not adversely affect the assurance baseline.

Re-evaluation refers to the evaluation of a changed TOE, such that the developer could not (or chooses not to) demonstrate that changes to the certified TOE do not adversely affect the assurance baseline.

Re-assessment refers to the evaluation of a previously certified TOE against a changed threat environment.

Figure 2.1 and 2.2 show the primary paths through assurance continuity. The starting point is when a change is made to the certified TOE [box 1]. This change might be a patch designed to correct a discovered flaw, an enhancement to a feature, the addition of a new feature, a clarification in the guidance documentation, or any other change to the certified TOE. For the specific case of re-assessment, no change has been made to the certified TOE but new threats or attack techniques are considered.

Figure 1: General process of Assurance continuity


1 Change is made to certified TOE
2 Evidence is Updated
IAR Created and submitted to scheme
3 Security Impact Of Change
minor
major
4 If applicable, the Evaluator performs Analysis and testing and creates partial ETR.
5 Certificate reissued with Addendum made to Certificate listing
Maintenance Report issued
6 Evaluator performs Analysis and testing
Applies other Assurance criteria
Creates ETR
7 New Certificate issued
Maintenance Report Issued
New Certified TOE

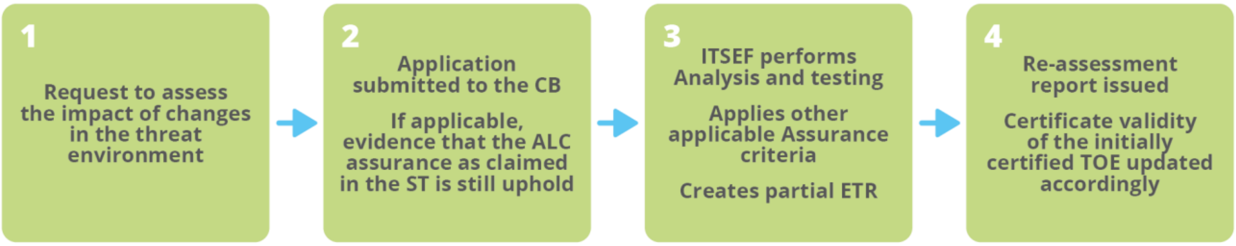
As a result of this change, a judgement needs to be made in regard to its resulting impact on assurance [box 2]. This includes an analysis of the evaluation evidence that would have to be updated to reflect the change, and regression testing of the code to be sure that it works when incorporated into the TOE. The basis for making this judgement is called impact analysis, which is performed by the TOE developer and recorded in an Impact Analysis Report (IAR); see Section 5 for more detail on the content of the IAR.

The certification body (CB) uses the IAR to determine whether [box 3] each of the changes has a minor or a major impact on assurance and is therefore considered requiring or not re-evaluation. It should be noted that a CB might use factors other than whether the changes are major or minor (e.g. elapsed time since certification).

If the CB agrees that the changes to the TOE are of minor impact, then it may be necessary (if there have been changes to the assurance measures in the development environment) for a ITSEF to [box 4] perform a subset evaluation of those assurance measures, and provide the certification body with a partial ETR covering those assurance components that were affected. Once the CB is in agreement that the assurance baseline has not been adversely affected, then [box 5] an addendum to the certification listing is created, and a Maintenance Report is produced from the IAR and made publicly available where it will serve as an addendum to the certification report of the original certified TOE and provided in an re-issued certificate for the changed ICT product.

If the CB finds that the change has a major impact on the assurance baseline, then the changed TOE must undergo re-evaluation in order for it to have an associated certification. This evaluation [box 6] makes maximum use of previously generated evidence, as well as the IAR, resulting in [box 7] a new ETR and hence the maintenance report is indeed a new certification report; in addition, the certification body issues a new certificate. This new certified TOE will then serve as the baseline against which future changes will be compared [back to box 1].

Figure 2: Re-assessment


1
Request to assess the impact of changes in the threat environment
2
Application submitted to the CB
If applicable, evidence that the ALC assurance as claimed in the ST is still uphold
3
ITSEF performs Analysis and testing
Applies other applicable Assurance criteria
Creates partial ETR
4
Re-assessment report issued
Certificate validity of the initially certified TOE updated accordingly

Where there is a request to assess the impact of changes to the threat environment on a certified TOE, a re-assessment request is submitted to the certification body [box 2]. No IAR is needed, but evidence that the assurance on the development environment is still uphold should be provided at this stage if available to avoid unnecessary evaluation work. The TOE then goes through evaluator analysis and testing [box 3]. Only the assurance activities impacted by the evolution of the threat environment are re-opened, namely the AVA_VAN family, and, if sufficient evidence could not be provided, the ALC class as well.

2.3.1 Process Description

The Assurance Continuity process can be defined in terms of the necessary inputs, actions and outputs that result in an update to the certified products list, to reflect:

1. the assurance gained for the changed TOE, or,
2. the impact on certificate validity for the initially certified TOE.

To achieve aim 1, Assurance Continuity provides a mechanism which enables developers to analyse the effect of changes and present their findings to the CB. This means that when a change occurs, developers must conduct relevant action items in order to determine whether the assurance baseline has been adversely affected. This process places an obligation on the developer to maintain all developer evidence (recording sufficient information in the IAR about changes to documentary evidence would be considered maintaining that evidence), conduct and record appropriate testing and confirm that previous analysis results have not been affected by changes to the TOE. Section 4: Performing an Impact Analysis further describes these types of activities. The Assurance Continuity process is described below.

In order for a CB to review the developer’s analysis, and in order to begin the process, the developer must ensure that the following inputs are available to the CB (the authority will most likely already have some of these inputs):

- Certificate for the TOE (including existing maintenance addendum)
- Certification Report
- Evaluation Technical Report
- Security Target for the certified TOE
- Impact Analysis Report (IAR)

Once the CB is satisfied that it has the required inputs, it will proceed with a review of the IAR and other relevant inputs in order to determine what impact the changes described in the IAR have on the assurance baseline.

The review process performed by the CB will most likely involve consultation with the developer and this consultation should result in a complete and consistent IAR. That is, the analysis recorded is complete and the IAR meets all requirements for content and presentation (see Chapter 5), to the satisfaction of the CB.

The IAR review is conducted in accordance with this annex and with any relevant guidance documentation that may be issued by the CB, and a key focus of this review is to determine whether the changes (to the TOE, the ICT environment and/or the development environment) can be considered major or minor, based on their apparent impact on the assurance baseline.

There are two possible outcomes from the IAR review:

i. The CB determines that the impact of changes on the assurance baseline are considered minor and the certificate maintenance addendum is subsequently updated to show that the certificate also applies to the maintained TOE. Section 2.3.2 provides further details regarding the certificate maintenance process.
ii. The CB determines that the impact of changes on the assurance baseline are considered major and the certificate maintenance addendum will not be updated. Such changes would need to be considered during re-evaluation. Section 2.3.3 provides further detail regarding the re-evaluation process.

Once this determination is made, the CB will inform the developer of the outcome. In either case, major or minor, the CB will record the underlying rationale for their decision in accordance with it quality assurance processes. These records may be also made available, where applicable, for the peer assessment process.

2.3.2 Handling of minor changes

The purpose of Assurance Continuity – Handling of minor changes is to allow for minor changes (those that can be shown to have little or no affect on assurance) to be made to a certified TOE, the ICT environment and/or the development environment, and have the resulting TOE version recognised as maintaining the same level of assurance as the certified TOE.

If the impact of changes to the TOE are considered to be minor, then the CB must also determine that the scope of any changes to the development environment do not have a follow-on effect on any assurance components outside of the development environment. For any changes to development environment assurance measures, it is necessary to have an ITSEF conduct a partial evaluation (see Section 2.3.2.1) of the applicable assurance components in the Security Target. Subsequent to the successful completion of any such partial evaluation, an updated maintenance addendum (see Section 2.3.2.2) and a Maintenance Report (see Section 2.4.2.3) are published on the evaluation authority's Certified Products List. The complete IAR is considered an output shared only between the developer and the CB.

2.3.2.1 Evaluating changes to the development environment

An ITSEF performs a partial evaluation, focussing only on those development environment assurance components for which the assurance measures have been modified. The ITSEF conducts this evaluation in the same way that they would normally perform a CC evaluation for that functionality, and produces a partial ETR that provides sufficient evidence to the evaluation authority that the assurance baseline has been preserved, for those changes to the development environment.

The ITSEF shall be selected in accordance with the assurance level associated to the evaluation.

2.4.2.2 Certificate maintenance Addendum

The certificate maintenance addendum serves as an addendum to the certificate for a certified TOE that lists the changed TOEs derived from that certified TOE.

Information required in the addendum is as follows:

- Unique TOE identifier for each changed TOE related to the certified TOE.
- Reference to the Security Target associated with the cahnged TOE (note that if the only change to the Security Target is to the version of the TOE then the original Security Target may be referenced).
- Reference to the Maintenance Report, which should be publicly available.

2.4.2.3 Maintenance report

In the case of a certificate maintenance, the maintenance report is considered to be an addendum to the certification report for the certified TOE. It provides details of the changes made to the certified TOE that have been accepted.

The information contained in the maintenance report is essentially a subset of the IAR content. The following sections of the IAR should be included in the maintenance report:

1) Introduction
2) Description of changes
3) Affected developer evidence

The content of each of these sections is described in Section 5 Impact Analysis Report. These sections may be sanitised when reproduced in the maintenance report by the removal or paraphrase of proprietary technical information if required.

The maintenance report should also contain a reference to the certification report for which it is an addendum.

CBs may wish to provide users with useful information in regard to a changed TOE. Such information could also be included in the maintenance report.

2.4.3 Re-evaluation

When a change to a certified TOE has been determined to be of major impact, the implication is that a more concerted analysis, and by an independent evaluator, is required to assess the assurance of the changed TOE. A re-evaluation is performed in the context of an earlier evaluation, reusing any results from that earlier evaluation that still apply.

It is possible that the developer may opt directly for re-evaluation without establishing an IAR (for example, if the changes are so substantial that the changed TOE bears only a minimal resemblance to the evaluated TOE). Alternatively, even with substantial changes, the developer still may have conducted a security impact analysis of the differences between the changed TOE and the evaluated TOE.

If an IAR has been provided, this would be used as the basis for identifying those parts of the changed TOE remaining unchanged from the previously-evaluated TOE. As with all evaluations, analysis that has already been performed on parts of a TOE that remain unchanged need not be performed again, thereby maximizing the amount of results of previous effort that can be re-used. To this end, the new ETR is derived from the ETR of the original TOE.

At the completion of the evaluation of the changed TOE, a new ETR is produced, along with a certification report that constitutes the maintenance report, and certificate for the changed TOE. This changed TOE becomes the updated basis for any future changes that might be made.

2.4.4 Re-assessment

When the threat environment has changed since the initial certification of a TOE, the certificate holder may want the TOE's resistance to be re-assessed. Re-assessment is performed by the same evaluator who performed the initial evaluation, reusing all results from that earlier evaluation that still apply. Only tasks pertaining to the AVA_VAN family are reopened, as well as, when relevant, those of the ALC class for which sufficient evidence that they are still fulfilled cannot be provided.

When updating the vulnerability analysis of the product, the ITSEF may consider the following:

- the list of potential vulnerabilities established during the initial evaluation is reused to update the vulnerability analysis. Attack methods and attack potential can evolve over time, thus the attack ratings may be changed from the initial certification. New penetration testing may also be performed to assess vulnerabilities initially considered as residual.
- new potential vulnerabilities which were not addressed during the initial certification, and associated attack methods are identified through examination of publicly available sources of information (see CEM work unit AVA_VAN.*-3) and any other evaluation evidence (see CEM work unit AVA_VAN.2-4 and higher) These new potential vulnerabilities are used to update the vulnerability analysis in accordance with the initial AVA_VAN level.

As re-assessment is based on the initial Security Target, no change to the security problem can be made and only new or evolved attack techniques are covered.

At the completion of the re-assessment of the TOE, a new ETR is produced, along with a re-assessment report for the reassessed TOE.

The validity of the initial certificate is then updated according to the following table:

Table 1: Impact of re-assessement results on certificates

Re-assessment results	Impact on the certificate
Positive[66]	The validity of the initial certificate is extended into the renewed certificate.
Negative	The new AVA_VAN level reached by the re-assessed TOE is indicated into a re-issued certificate, and the previous certificate is archived.

When the validity of the certificate is extended, the new validity period is established in respect of the applicable rule adopted by the scheme.

3 CHARACTERISATION OF CHANGES

The CB examines the changes described in the Impact Analysis Report in order to determine their impact upon the assurance of the certified TOE.

A minor change is one whose impact is sufficiently minimal that it does not affect the assurance to the extent that the evaluator activities need be independently reapplied (although the developer is expected to have tested the changes as part of his standard regression testing) or a change to the development environment in which the change can be shown to have no follow-on effect on the other assurance measures that were in place at the time of the original evaluation.

By contrast, a change deemed major has an impact that is substantial enough that it does affect the assurance (except as noted above for the development environment) and would consequently warrant independent re-application of the evaluator activities.

Therefore, minor changes are addressed under certificate maintenance, which is performed solely by the developer, while major changes are addressed under re-evaluation, which is performed by the evaluator.

It is important to note the difference between a change's impact upon the certified TOE and a change's impact upon the assurance of the certified TOE. A given change that is widespread and affects many parts of the TOE might have no effect upon the assurance of the TOE, or it could have far-reaching effects upon the assurance of the TOE. Similarly, a given change that affects only a very small part of the TOE might have no effect upon the assurance of the TOE, or it could have far-reaching effects upon the assurance of the TOE.

It is impossible to predict all possible changes to all possible TOEs and, therefore, to identify the impact of all possible changes (and whether a given possible change is minor or major). Consequently, there is no fixed method for identifying whether the security impact of a change is major or minor. The following offers a general guideline on the differences between major and minor changes, and also offers examples of exceptions.

3.1 Typical minor changes

Minor changes typically consist of changes to the TOE that have no effect on any claims about the TOE. Examples of minor changes that are therefore suitable to be addressed under certificate maintenance are:

1) Changes to the IT environment that do not change the certified TOE. For example, a change to the underlying hardware (where the hardware is not part of the TOE) or to software parts of the product that are outside the TOE boundary would likely be minor if the interface remains unchanged. However if the interface also changes, then it is likely a major change.
2) Changes to the Certified TOE that do not affect the assurance evidence. For example, if a TOE has been certified to EAL1, a change to the source code and/or hardware schematics would not have an impact upon the assurance documentation. Nevertheless, the developer would have tested the changes as part of the standard regression testing.
3) Editorial changes (grammatical, typographical, formatting) to any of the assurance evidence. For example, editorial changes to a functional specification that provide additional clarification would probably be minor. However, if a PP were to specify exact compliance as the degree of conformance, then even an editorial change to the ST's security objectives statements or environment description would be major.
4) Changes to Development Environment. A change to the development environment that can be shown to have no follow-on effect on other assurance measures would typically be a minor change. An example of this

[66] Positive here means that the TOE is re-assessed conformant to the same AVA_VAN component as initially claimed in the Security Target.

would be where a developer has passed a certification that claimed ALC_CMC.2 and for whatever reason changed Configuration Management Tool. If the developer can provide, in the Impact Analysis Report, a convincing rationale that this process does not have follow-on effects on the other assurance measures that were in place originally, then this could be considered minor.

5) Changes to the ST front matter. A change to the ST's identification or to the TOE identifier (e.g. product name change) would be minor. If any of the statements of Threats, OSPs, Assumptions, or Security Objectives change, without necessitating a change to the Security Requirements, these would likely be minor changes. If, however, any of the requirements statements do change, these would be major changes.

3.2 Typical major changes

Major changes typically consist of changes to the claims about the TOE and may (yet need not) result in changes to the TOE. Examples of major changes that are therefore suitable to be addressed under re-evaluation are:

1. Changes to the set of claimed assurance requirements. This includes both the addition of new assurance measures and the deletion of existing assurance measures.
2. Changes to the set of claimed functional requirements. This would likely change the TOE boundary, which would have to be re-assessed for correctness and soundness under re-evaluation.
3. A set of minor changes that together have a major impact upon the security. Although changes might be of minor impact in isolation, the collection of minor changes could have a major security impact. The combination of these would have to be re-evaluated.

It should be noted that a bug fix has no predictable extent of change to the certified TOE, nor a predictable effect upon the assurance of the certified TOE. Therefore, a "bug fix" might constitute either a major or minor change.

4 PERFORMING AN IMPACT ANALYSIS

4.1 Input

The following are inputs to the impact analysis process:

a) developer evidence associated with the Certified TOE;
b) change(s) description (probably generated from life cycle quality processes and procedures).

4.2 Preliminary work

Security categorisation of the TOE may be used as a tool to help assess if a change is within the scope of maintenance. For example, when a change is described in an impact analysis, the security categorisation may be consulted to identify the influence of the change on the developer evidence provided in the assurance baseline.

Security categorisation may include any security relevant development tools, secure delivery procedures, developer security procedures, development life-cycle activities, or the security relevant procedures affecting the use or administration of the configuration management system.

It should be noted that any additions to the TOE will need to be security categorised, according to the chosen approach, and any modified portions may need to have their security categorisation reviewed.

4.3 Steps in performing the impact analysis

During maintenance, it is the developer's responsibility to confirm that content and presentation verdicts for modified developer evidence can still be met. Having identified the effect of the change on the developer evidence, the developer is then able to conclude the security effect of the change.

Step 1 - Identify Certified TOE

Determine the developer evidence provided for the certified TOE assurance baseline, including the certified TOE. All changes are applied against this baseline.

Step 2 - Identify and describe change(s)

Describe the change(s) to the product with regard to the product associated with the certified TOE.

Identify and describe the change(s) to the development environment with regard to the development environment of the certified TOE.

These changes are listed to the level of detail necessary to understand what was done, but not necessarily how it was done.

Step 3 - Determine impacted developer evidence
The objective of this step is to determine, considering each change from the previous step, which items of the developer evidence need to be updated. This step should be conducted in a systematic way, considering in turn each assurance component included in the assurance package for the certified TOE, the effect of the change on the assurance component and the evidence provided for that component. The following list can be used to facilitate such an approach.

For a change to the product, the following aspects should be considered:

a) Has it affected the Security Target?
b) Has it affected the reference for the TOE?
c) Has it affected the list of configuration items for the TOE?
d) Has it affected any of the TSF abstraction levels, that is, the functional specification, the TOE design, or the implementation representation?
e) Has it affected the architectural description (if the assurance baseline includes a component from the ADV_ARC family)?
f) Has it affected the mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design (if the assurance baseline contains a component from the ADV_TDS family), and to the implementation representation (if the assurance baseline contains a component from the ADV_IMP family)?
g) Has it affected the guidance documentation (if the assurance baseline includes a component from the AGD class)?
h) Has it affected the testing documentation, that is, the analysis of test coverage, the analysis of the depth of testing or the test documentation (if the assurance baseline includes a component from the ATE class)?
i) Has it affected the vulnerability analysis?

For a change to the development environment, the following aspects should be considered:

a) Has it affected the Security Target?
b) Has it affected the CM documentation?
c) Has it affected the delivery procedures (if the assurance baseline includes a component from the ALC_DEL family)?
d) Has it affected the procedures necessary for the secure acceptance of the delivered TOE, secure installation of the TOE, and secure preparation of the operational environment?
e) Has it affected the developer security procedures (if the assurance baseline includes a component from the ALC_DVS family)?
f) Has it affected the flaw remediation procedures (if the assurance baseline includes a component from the ALC_FLR family)?
g) Has it affected the life cycle model (if the assurance baseline includes a component from the ALC_LCD family)?
h) Has it affected the development tools (if the assurance baseline includes a component from the ALC_TAT family)?
i) Have there been changes to the manufacturing process (in particular for hardware components)?

The impacts on all the developer evidence should be considered, based on the change description, in order to check that all potential impacts have been identified.

Note that the ST is likely to be affected, even if it is substantially similar to the original ST. If the TOE has changed, it would include at least a change to the TOE version number.

Previous versions of the IAR may be used as input to this analysis.

For some developer action elements this determination may be simple (e.g. a new graphical user interface for the changed TOE, to be delivered in the same manner used for the TOE, will not have an adverse impact on ALC_DEL), while for other requirements it may be more difficult (e.g. has the TOE design for the user interface subsystem changed through the introduction of the new GUI and the effect on the material provided for ADV_TDS?

The output of this step is a list of affected developer action elements.

Step 4 - Perform required modifications to developer evidence.
The objective of this step is to determine how each of the affected developer evidence (identified during the previous step) should be modified in order to address the corresponding content and presentation of evidence elements. It is sufficient to collect together changes required to developer evidence before actually implementing those changes.

Testing (regression testing) could be required to update the evidence. For instance, the developer may repeat a sample of the developer tests delivered for the evaluation.

Regarding the IAR, sufficient information about how the developer testing was updated would be required, commensurate with the testing components in the assurance baseline. If new tests were written to address a change, these are identified, with the test purpose, in the impact analysis report. However, the details of the test in terms of providing the test scripts including the individual test steps of the test, are not required.

If the change to the TSF is "invisible" at the lowest TSF abstraction available (e.g., the lowest level of TSF decomposition is represented by the ADV_TDS.2 component, and some source code is changed during maintenance, but the changes do not require modification to the subsystems in the TOE design), then it suffices for the developer to show how the change was tested, and provide associated rationale in the IAR.

The output of this step is a list of updated evidence (this could take the form of a list of changes to the evidence - where, why, what).

Step 5 – Conclude

Determine the overall impact of the identified changes on the assurance of the certified TOE. Conclude: minor or major impact.

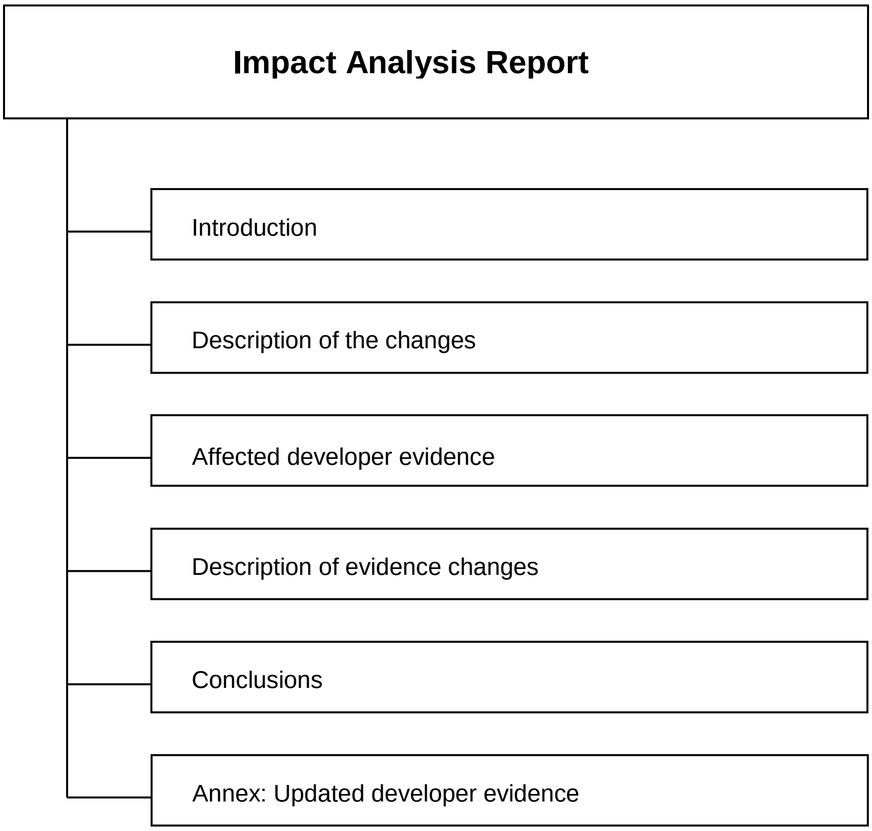
4.4 Outputs

a) Impact Analysis Report (IAR);
b) Updated developer evidence.

5 IMPACT ANALYSIS REPORT (IAR)

This section describes the minimum content of the IAR. The contents of the IAR are portrayed in Figure 5.1; this figure may be used as a guide when constructing the structural outline of the IAR document. The IAR is a required input for the maintenance process.

Figure 2: Impact Analysis Report


Impact Analysis Report
Introduction
Description of the changes
Affected developer evidence
Description of evidence changes
Conclusions
Annex: Updated developer evidence

5.1 Introduction

The developer shall report the IAR configuration control identifiers. The IAR configuration control identifiers contain information that identifies the IAR (e.g. name, date and version number).

The developer shall report the current TOE configuration control identifiers.

The TOE configuration control identifiers identify the current version of the TOE that reflects changes to the certified TOE.

The developer shall report the configuration control identifiers for the ETR, certification report, and certified TOE. These configuration control identifiers are required to identify the assurance baseline and its associated documentation as well as any other changes that may have been made to this baseline.

The developer shall report the configuration control identifiers for the version of the ST related to the certified TOE.

The developer shall report the identity of the developer. The identity of the TOE developer is required to identify the party responsible for producing the TOE, performing the impact analysis and updating the evidence.

The developer may include information in relation to legal or statutory aspects, for example related to the confidentiality of the document.

5.2 Description of the change(s)

The developer shall report the changes to the product. The identified changes are with regard to the product associated with the certified TOE.

The developer shall report the changes to the development environment. The identified changes are with regard to the development environment of the certified TOE.

5.3 Affected developer evidence

For each change, the developer shall report the list of affected items of the developer evidence. For each change to the product associated with the certified TOE or to the development environment of the certified TOE, any item of the developer evidence that need to be modified in order to address the developer action elements shall be identified.

5.4 Description of the developer evidence modifications

The developer shall briefly describe the required modifications to the affected items of the developer evidence. For each affected item of the developer evidence, the modifications required to address the corresponding content and presentation of evidence elements shall be briefly described.

5.5 Conclusions

For each change the developer shall report if the impact on assurance is considered minor or major. For each change the developer should provide a supporting rationale for the reported impact. In the event that the change is to the development environment, the rationale will show that there is no follow-on impact on other assurance measures.

The developer shall report if the overall impact is considered minor or major.

The developer should include a supporting rationale, taking the culmination of changes into consideration.

5.6 Annex: Updated developer evidence

The developer shall report for each updated item of developer evidence the following information:

-the title;
-the unique reference (e.g. issue date and version number).

Only those items of evidence that are notably changed need to be listed; if the only update to an item of evidence is to reflect the new identification of the TOE, then it does not need to be included.

38. ANNEX 12: PROCEDURE FOR CONDUCTING A PEER ASSESSMENT

PURPOSE

This annex describes the applicable procedure for peer assessments.

PARTICULAR STATUS

None.

CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE

Chapter 22, PEER ASSESSMENT.

1 SCOPE

This annex describes the applicable procedure for peer assessments. The procedure consists of four phases: preparation, site visit, reporting, and adoption of a report.

The procedure only defines the process to be followed. In order to be as comprehensive and objective as possible, checklists shall be further developed in cooperation with the ECCG to assist the peer assessment team. These checklists will contain a common understanding of state of the art[67] and operating practices.

This procedure covers three types of peer assessments:

1. Type 1: When a Certification Body (CB) performs certification activities at the AVA_VAN.3 level;
2. Type 2: When a CB performs certification activities related to a Technical Domain;
3. Type 3: When a CB performs certification activities above the AVA_VAN.3 level according to a Protection Profile defined specifically for this usage and annexed to the EUCC scheme.

Any differences between Types 1 and Type 2 above are identified within this procedure. Type 3 will need further development when such Protection Profiles will be developed.

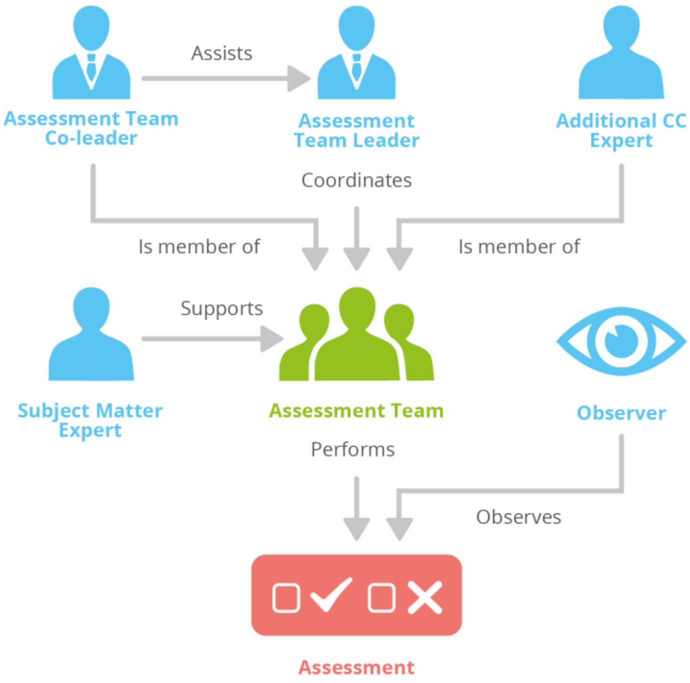
2 OVERVIEW

The primary assessment team shall consist of two Common Criteria (CC) experts (Leader and co-Leader) selected from two certification bodies (CBs) issuing certificates at the assurance level ‘high’ of the CSA.

This primary assessment team may be extended with additional CC experts from other or the same CBs, and in the case of a delegation of the issuance of certificates or of prior approval of certificates, an expert from the concerned NCCA may be associed to the selected CB expert into the team.

[67] As discussed in cooperation with the ECCG and/or relevant subgroups.

Figure 1: Assessment team organisation



For a Type 2 peer assessment the primary assessment team shall be selected from CBs acting in the related Technical Domain.

Each CC expert in the assessment team shall have a minimum of the following skills/experience:

1. two years as a certifier at a CB, and acting in the relevant Technical Domain(s), if applicable;
2. participation to the assessment of the capabilities of an ITSEF performing evaluation for the CB in support of the authorization of the CB, as defined by Chapter 7, NOTIFICATION AND AUTHORISATION OF CAB, FUNCTIONING OF CAB AND SUBCONTRACTORS.

For a Type 2 peer assessment, the peer assessment team can be assisted by subject matter experts in the Technical Domain(s) concerned. Those experts may be certifiers themselves, but that is not essential.

It is also highly recommended that the peer assessment team members have participated in previous peer assessments either as observers or team members. Ideally these should be peer assessments performed under the EUCC scheme, but peer assessment experience under other Mutual recognition arrangements such as the SOG-IS MRA, or the CCRA, is also of benefit.

The peer assessment can be observed by observers proposed by other NCCAs.

The peer assessed CB may present to the ECCG any concern it has about the choice of the peer assessment team members and observers, for example in case of a conflict of interest

The peer assessment activities will be carried out in four phases.

The preparation phase will involve the review of the CB documentation by the members of the peer assessment team in order to become familiar with the CB's policies and procedures.

The site visit phase will consist of a two weeks visit by the peer assessment team to the CB in order to assess the CB's technical competence, and where applicable of ITSEFs performing evaluations. The exact duration of site visit will depend on the possible reuse of existing peer assessment evidence and results, and, for Type 2 assessment, on the number of ITSEFs and on the number of Technical Domains the CB issues certificates for.

The peer assessment will include a reporting phase: he assessment team will document their findings in a peer assessment report delivered to the ECCG.

The peer assessment will conclude with the adoption of an opinion by the ECCG of the outcome of the peer assessment.

3 SCHEDULING PEER ASSESSMENT ACTIVITIES

In accordance with the planning established by the ECCG, and taking into consideration the possible priorities indicated in Chapter 22, PEER ASSESSMENT, the ECCG shall notify the CB of the peer assessment, and will task a peer assessment team to perform the peer assessment.

The peer assessed CB shall submit the required number of candidate products for which the CB has followed the evaluation projects, for review by the peer assessment team. In general the candidate products shall cover all technical aspects of the audit.

Where certification above AVA_VAN.3 for ICT products that are not covered by a Technical Domain has been established according to specific Protection Profiles certified under this scheme for this purpose, at least one ICT product certified according to these Protection Profiles shall be included in the list of candidate products.

For a Type 2 peer assessment, the CB shall submit at least one product per Technical Domain per considered ITSEF, for which the CB has followed the evaluation project, for review by the assessment team, and supply details of every ITSEF that it considers to be qualified to evaluate at the higher level in that technical domain.

Requirements for minimal number of products are summarized in the following Table.

Table 1: minimal number of products

Evaluated products	Type 1	Type 2
Minimal number of products	2	min. 1 per Technical Domain and per each ITSEF*

* EXAMPLE:

1. number of Technical Domains requested: 2
2. number of ITSEFs applying for a higher level of evaluation on the 2 Technical Domains: 2
3. minimal number of products evaluated under the shadow certification: 2 x 2 = 4

The requested information and the list of candidate products (and ITSEFs) shall be provided by the peer assessed CB to the peer assessment team within one month after the notification by the ECCG.

The assessment team will arrange the dates for the peer assessed CB and where applicable ITSEF(s) site visit(s).

4 RESPONSIBILITIES OF THE PEER ASSESSED CB

The peer assessed CB shall provide the following documentation:

- a full description of its scope, organization and operation, including:
  - the title, address and principal point of contact;
  - its role according to Article 56;
  - the accreditation decision for the CB;
  - the procedures for certification;
  - where applicable, the procedures for the prior approval for each individual certificate or the requirements from a general delegation;
  - the rules applying within the peer assessed CB and its internal or external testing facilities (ITSEFs) to the protection of protected other sensitive information;
  - the titles and addresses of the ITSEFs participating in the activities and their status (commercial or governmental);
  - the procedures by which the peer assessed CB ensures that ITSEFs apply the evaluation criteria and methods correctly and consistently and protect the confidentiality of sensitive information involved;
- the latest list of the certificates issues by the peer assessed CB for the last five years;
- two or more certificates and Certification Reports issued which are selected by the peer assessment team;
- where reuse of a previous peer assessment results is proposed, associated results, under the conditions of Chapter 22, PEER ASSESSMENT.

In addition, all relevant information about the quality management system that has been implemented by the CB in order to obtain accreditation by its NAB shall be provided. It should be noted that this information is provided for informative purposes and that the content of this information is not the focus of the peer assessment. Any deviations from processes described in these documents that are found shall however be reported.

All written documentation and communications for the peer assessment activities must be provided in English at least 4 weeks before the audit date.

For a Type 2 peer assessment, the CB shall provide a list of all ITSEFs that perform evaluations for that domain and a description of the evidence used when assessing the competences of these ITSEFs.

During the site visit, English will be spoken, unless the CB and the peer assessment team unanimously agree upon another language.

One part of the peer assessment activities during the site visit will involve a review of at least one evaluation that has been completed or is close to being completed within the CB. (In the case of an application for a higher level in a Technical Domain (Type 2 defined above) the evaluation must be for a product within that domain and involve appropriate attack methods/vulnerability search at the associated level).

Although the evaluations for chosen products submitted for consideration need not be entirely complete, there must be records showing that significant evaluation analysis and certification activities have been performed, and that the majority of the evaluation report (including at least one vulnerability analysis round) has been delivered to and analysed by the certification team.

In addition to the selected products, the CB may also provide the peer assessment team with information on (up to) another two evaluations which were completed in the 12 months prior to the start of the peer assessment activities. If the peer assessment team has sufficient time and resources, they will review these evaluations during their site visit and, if they are found to be compliant with the EUCC scheme requirements, will take them into consideration within the peer assessment report.

The CB is responsible for preparing, documenting and providing general information on the candidate products. This information will be provided to the peer assessment team for their review and selection and shall include:

- a brief overview of the product,
- the status of the evaluation (if not completed, then indicate what parts of the evaluation have been completed and what remains to be done),
- the target EAL and AVA_VAN levels (and augmentation, if any),
- any Protection Profile compliance claims.

The peer assessment team will select at least one candidate evaluation(s) to be assessed during the site visit(s) of the CB and where applicable of the ITSEF(s).

The CB will identify a Point of Contact who will be the individual responsible for facilitating the peer assessment activities and for interacting with the assessment team leader.

The CB Point of Contact is responsible for:

- Coordinating the site visit(s) dates and location(s) with the peer assessment team,
- Delivering the CB materials to the peer assessment team during the Preparation Phase at least 4 weeks before the audit date,
- Coordinating any required ITSEF(s) visits with the peer assessment team,
- Arranging all necessary approvals to allow the peer assessment team to perform the CB and ITSEF(s) site visits and to have access to all information required to complete the peer assessment activities,
- Coordinating the peer assessment agenda for the CB, including scheduling certifiers for peer assessment team interviews and briefings, ensuring the availability of materials to be reviewed during the site visit, etc.,
- Providing the peer assessment team with the ability to have copies and printouts made for use during the site visit;
- Providing secure storage, if required, for the peer assessment team’s documents (e.g. lunchtime, overnight);
- Being generally available to answer questions and resolve issues that may arise during the site visit,
- Coordinating the review of the peer assessment report by CB representatives,
- Providing feedback to the peer assessment team leader on the peer assessment draft report.

The CB must have private room(s) available that is (are) large enough to accommodate the peer assessment team and CB personnel during the site visit(s). Such room(s) will serve as the meeting room throughout the site visit. Accessibility to records and CB personnel will be needed throughout the site visit in the meeting room.

5 RESPONSIBILITIES OF THE PEER ASSESSMENT TEAM LEADER

One member of the peer assessment team will be designated the team leader. The team leader is responsible for the following tasks:

- Coordinating the receipt of materials from the CB,
- Coordinating the decision regarding the selection of the candidate products (and ITSEFs) and notification to the peer assessed CB,
- Drafting the site visit agenda (and for acceptance as a certificate producer at a higher level in a Technical Domain (Type 2) the selected ITSEF(s) to visit), and coordinating it with the CB,
- Coordinating and completing the peer assessment draft-report at the end of the site visit,
- Delivering the peer assessment final report to the ECCG, ,
- if necessary, monitoring the CB’s resolution of outstanding issues resulting from the peer assessment.

6 PREPARATION PHASE

The peer assessment team should begin preparation approximately four weeks before the site visit. The peer assessed CB shall provide the peer assessment team with access to all written policies and operating procedure documents four weeks before the site visit. Electronic and/or hardcopy documentation have to be provided, depending on the preference of the peer assessment team members and nature of documentation needed. The peer assessment team should focus their review of the documentation on gaining an understanding of the CB’s standard operating procedures.

The peer assessment team leader will coordinate the review of materials during the preparation phase. If there is a large amount of material to be reviewed, the team may divide it so that members review different portions of the documentation. The team leader will also draft and finalize the site visit(s) agenda, with input from the team members, at the conclusion of the preparation phase. The site visit(s) agenda must be forwarded to the peer assessed CB no later than one week before the site visit(s). It is recommended that the peer assessment team leader should maintain close contact with the CB Point of Contact during the preparation phase to keep the CB informed of areas that will require further investigation during the site visit.

Previous peer assessment results with associated results may be proposed by the CB for consideration by the peer assessment team.

7 SITE VISIT PHASE

7.1 Determine that the constitution and procedures of the CB comply with the general requirements of the EUCC scheme

A checklist shall be used to determine if the processes that the CB uses to provide its certification services are sufficient to ensure effective oversight of evaluations and to ensure that successful certifications comply with the Common Criteria and the Common Evaluation Methodology.

The CB shall provide any relevant information associated to its accreditation to support this determination.

Where the peer assessment team decides to check some procedures of the CB, this should occur before the assessment process commences. Nevertheless, the peer assessment team should check that the CB is applying its procedures. This can be done at the site visit (see below) for the particular certifications being assessed.

7.2 Perform the peer assessment

For a Type 1 peer assessment, the peer assessment team should allocate one full week (5 working days) for the site visit. If the peer assessment is completed in a shorter period of time, the team will not need to stay the full week.

For a Type 2 peer assessment, the peer assessment team should allocate two full weeks for the site visit(s). If the peer assessment is completed in a shorter period of time, the team will not need to stay the full two weeks.

The peer assessment team shall have access to all evaluation and certification documentation that was used by the CB during its certification process and especially when reviewing the evaluation documentation, and shall be permitted to observe all activities carried out during such review. If an evaluation team/certifier meeting occurs during the site visit, the peer assessment team should observe the meeting.

The peer assessment team should not completely review the work of the ITSEF, which may be covered by its accreditation under ISO/IEC 17025. However, the peer assessment team should assess whether the deliverables available to the CB are of sufficient quality to allow the CB to determine that the evaluation was conducted in accordance with the appropriate methodology.

For a Type 2 peer assessment, the peer assessment team will make a determination of ITSEF technical competence by:

- visit of technical lab in the ITSEF site,
- interviews with evaluators on technical items related to the Technical Domain and its specific attack methods.

Findings corresponds either to

- non-conformities that are linked to a requirement from the applicable checklist or to common understanding of state of the art and operative practices that are not met (or not fulfilled). The latter will be discussed with the ECCG and could, where appropriate, be incorporated as a new item into the lists for use by future peer assessments.
- or observations that correspond to improvement proposals made by the peer assessment team, not directly linked to requirements from the checklist.

A non-conformity could be either critical or non-critical. A critical non-conformity challenges the reliability of the results established by the assessed CB. The peer assessment team shall analyse and describe the impact of each critical non-conformity.

At the end of the site visit, the peer assessment team should present the list of findings (at least the draft list of non-conformities associated to their criticality level) to the peer assessed CB, so that the assessed CB can establish a proposed action plan to cover the findings. The peer assessment team should provide the final list of non-conformities (associated to their criticality level) not later than 4 weeks after the site visit to the peer assessed CB.

If non-conformities have been identified, the CB may request the support of the peer assessment team for establishing an action plan associated to a timescale to implement the relevant measures.

8 REPORTING

The peer assessment team shall produce a report that summarizes and explains their findings.

The report should be agreed internally within the peer assessment team. If the peer assessment team cannot agree internally, then majority and minority opinions shall be included in the report.

CB’s disagreement on findings can be incorporated to the report, no later than one month after the report has been established.

The report shall also present the position of the peer assessment team on the relevance of proposed action plan to cover the findings, if this plan was submitted to the team prior to the delivery of the report to the ECCG. If evidence that cover critical non conformity is provided before issuance of the report, the team can reconsider the criticality of the non-conformity and shall document this change in the report.

The assessment team might include into its report relevant outcomes and findings from other peer assessments reused.

Findings from the peer assessment team included in the report shall be clearly identified, with a unique and unambiguous identifier.

The final report shall be produced within three months after the site visit and will be reviewed by the peer assessed CB prior to distribution to the ECCG.

For preparation of the final report the following steps will be followed:

1. the peer assessment team will prepare a draft report, including all findings, unresolved minor and major non-conformities detected during the peer assessment in the preparation phase and the site visit phase, and deliver it for comments to the assessed CB. (one months)
2. the assessed CB will comment the draft report, highlighting any points of disagreement and proposing changes to the report.(one month)
3. the peer assessment team will consider the comments received by the CB and produce a final report with possible revisions.(one month)

All three documents at points 1-3 will be delivered to the ECCG by the peer assessment team to give evidence of the final reporting phase of the peer assessment.

If any deviations of relevance for the NAB have been found, the NAB shall be informed.

The report shall provide one of three possible verdicts:

Pass: The CB has met all requirements and no measure is required.

Pass with controlled (minor) non-conformities: The CB has not met all requirements, but has provided a relevant actions plan and an acceptable timescale for correcting the non-conformities identified by the peer assessment team. There is no-remaining critical non-conformity identified in the report.

Fail: The CB has not met the requirements and has not provided a relevant actions plan and an acceptable timescale for correcting the non-conformities identified by the peer assessment team

The peer assessment team leader (or a suitable representative with full knowledge of the assessment) shall present the report to the ECCG, including any disagreement within the team of with the peer assessed CB. He/she shall present the findings of the team and its appreciation of how the measures proposed by the CB will solve the issues.

Where relevant, appropriate additions will be made to the assessment checklist to assist future peer assessment teams.

9 ADOPTION OF PEER ASSESSMENT REPORT

The following procedure is provided to guarantee adequate involvment of the assessed CB to demonstrate prompt resolution of non-conformities. The procedure also helps limiting the time for the adoption of the peer assessment.

1. The ECCG will request the ECCG subgroup dedicated to maintenance of the EUCC scheme to prepare an opinion to be adopted by the ECCG on the conducted peer assessment.

2. The ECCG subgroup will meet to discuss the result of the peer assessment (based on documents 1-3) and invite for the meeting the peer assessment team and the assessed CB. Following the meeting, one of the following proposals of opinion will be issued by the ECCG subgroup:

   - the final report from the assessment team is proposed to be adopted as it is;
   - an amended final report from the assessment team is proposed to be adopted.

   In the case of non-conformities, the opinion to be adopted by the ECCG will include a recommendation to the assessed CB to resolve such non-conformities with an indication of the duration allocated to this resolution. This duration should be limited to 2 months in the general case and should not exceed 6 months.

3. the ECCG subgroup will deliver to the ECCG:

   - the minutes of the meeting;
   - the proposed opinion to be adopted by the ECCG.

   The ECCG subgroup shall ensure that any feedback on non-conformities or recommedations received by the CB that underwent the peer assessment or the NAB will be forwarded along to the ECCG.

4. The ECCG will provide its opinion on the draft opinion. In the case of favourable opinion, the assessed CB will:

   a. either pass the peer assessment (if the draft opinion indicated a positive verdict of the peer assessment). The positive verdict will be published on ENISA website directly with the accompanying peer assessment findings.
   b. or be recommended to take the necessary actions to resolve the non-conformities in the allocated duration. The recommendation will not be published on the ENISA website.

   The ECCG could also request the ECCG subgroup to re-examine the peer assessment (GO TO POINT 2. again) only for one time.

5. When corrective actions are requested by the ECCG to the CB, following the implementation of the corrective actions, the assessed CB will issue a report to the ECCG subgroup within 2 months.

6. The ECCG subgroup will take a meeting within 2 months with the assessed CB and the assessment team to discuss the status of resolution of the non-conformities. The lack of a report from the assessed CB will not prevent the ECCG subgroup to have the meeting.

7. The ECCG subgroup will prepare an opinion to be adopted by the ECCG containing either a pass (successful correction of non-conformities) or a fail (residual non conformities already in place) and will deliver the proposed opinion and the minutes of the meeting to the ECCG.

8. The ECCG will establish its opinion based on the draft opinion and adopt the final result (including residual recommendation, or no recommendation for the CB). The ECCG will adopt the proposed opinion or adopt its own opinion, without recurring to further iterations with the ECCG subgroup. The opinion adopted by the ECCG will be published with all relevant documents on the ENISA website.

39. ANNEX 13: CONTENT OF A CERTIFICATION REPORT

PURPOSE

This annex details the content of a Certification Report.

The Certification Report is the source of detailed security information about the ICT product or protection profile for any interested parties. Its objective is to provide practical information about the ICT product or protection profile to consumers. The Certification Report need not, nor should contain protected information.

PARTICULAR STATUS

None.

CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE

Chapter 17, CONTENT AND FORMAT OF CERTIFICATES.

Based on the Evaluation Technical Report (ETR) established by the ITSEF, the issuer of a certificate shall establish a Certification Report associated to each certificate.

The Certification Report shall be the source of detailed information about the ICT product and how to securely deploy it, and shall therefore provide practical and publicly sharable information about the ICT product to end users and interested parties. The Certification Report shall at least contain the following sections:

1 EXECUTIVE SUMMARY

The executive summary shall be a brief summary of the entire report. The information contained within this section shall provide the audience with a clear and concise overview of the evaluation results and shall include the following information:

- name of the evaluated ICT product, enumeration of the components of the product that are part of the evaluation and version manufacturer or provider;
- name of the ITSEF that proceeded to the evaluation, and of subcontractors, where applicable;
- completion date of evaluation;
- reference to the evaluation technical report established by the ITSEF;
- brief description of the report results, including:
    - CC version/release used for the evaluation;
    - CSA assurance level achieved, CC assurance package including the AVA_VAN level achieved;
    - functionality;
    - summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated ICT product;
    - special configuration requirements;
    - assumptions about the operating environment;
    - where applicable, presence of an approved patch management mechanism;
    - disclaimer(s).

2 IDENTIFICATION

The evaluated ICT product shall be clearly identified with the inclusion of the following information:

- name of the evaluated ICT product;
- enumeration of the components of the product that are part of the evaluation;
- software version number;
- identification of any applicable software patches;

- hardware version number, including peripheral devices, where applicable;
- name and contact information of the manufacturer or provider;
- where applicable, applicable patch management mechanism;
- link to the website of the manufacturer or provider to access the Supplementary cybersecurity information for the certified ICT product in accordance with Article 55 of the CSA.

The information included in this section shall be as accurate as possible in order to ensure that a whole and accurate representation of the ICT product can be recreated for its use or for future evaluations.

3 SECURITY POLICIES

This section shall contain the description of the ICT product's security policy and shall contain the policies or rules that the evaluated ICT product must comply with and/or enforce. It shall include a reference and a quick description of the:

- manufacturer or provider vulnerability handling policy;
- manufacturer or provider assurance continuity policy.

Where applicable, such policy may include the conditions related to the use of a patch management mechanism, and this section shall then indicate that it is possible to apply the patch mechanisms according to this policy during the validity of the certificate.

4 ASSUMPTIONS AND CLARIFICATION OF SCOPE

This section shall contain information regarding the aspects of the environment/configuration in which the ICT product is expected to be used. The information shall include:

- usage assumptions that shall provide a baseline for the product during the evaluation, such as proper installation and configuration and minimum hardware requirements being satisfied;
- environment assumptions made about the ICT product during the evaluation;
- list and descriptions of the threats to the ICT product that have not been included in the evaluation.

The information included in this section shall be as accurate as possible in order to let end users make informed decisions about the risks associated with using the ICT product.

5 ARCHITECTURAL INFORMATION

This section shall include a high-level description of the ICT product and its major components, based on ADV_TDS subsystems design.

6 SUPPLEMENTARY CYBERSECURITY INFORMATION

A complete listing of the ICT product supplementary cybersecurity information shall be provided in respect of Article 55 of the CSA. All relevant documentation shall be noted with the version numbers.

7 ICT PRODUCT TESTING

This section shall include the following information:

- the testing facility that performed the evaluation
- the name and point of contact of the authority or body that issued the certificate including the responsible NCCA
- the name of the ITSEF which performed the evaluation, when different from the certification body
- an identification of the assurance type from the CSA (either ‘substantial’ or ‘high’) and (when available) related mark/label
- an identification of the used assurance components from CC Part 3
- security evaluation criteria and methodology used and their version
- the complete and precise settings and configuration of the IT product during the evaluation, including operational notes and observations if available;
- any Protection Profile that has been used, including the following information:
  - Protection Profile developer
  - Protection Profile name/identifier
  - certificate number
  - name of the certificate issuer and of the ITSEF
  - Assurance Package required for a product conforming to the Protection Profile

8 RESULTS OF THE EVALUATION AND INFORMATION REGARDING THE CERTIFICATE

This section shall include the following information:

- assurance level from the CSA reached (either 'substantial' or 'high');
- assurance requirements from CC Part 3 that the ICT product satisfies, including the AVA_VAN level;
- detailed description of the assurance requirements, as well as the details of how the product meets each of them;
- date of issuance and period of validity of the certificate
- Unique-ID of the certificate.

9 SUMMARY OF THE SECURITY TARGET

The Security Target shall be:

- included in the Certification Report;
- or referenced and summarised in the Certification Report and provided with the Certification Report for publication in association with it.

It may be sanitised by the removal or paraphrase of proprietary technical information: Annex 14: ST SANITISING FOR PUBLICATION defines the rules for sanitising a Security Target and describes the minimum content of the resulting document.

10 WHEN AVAILABLE, MARK OR LABEL ASSOCIATED TO THE SCHEME

When available, the mark or label associated to the scheme as defined by Chapter 10, MARKS AND LABELS may be inserted.

11 BIBLIOGRAPHY

The Bibliography section shall include all referenced documentation used as source material in the compilation of the certification report. This information shall include and is not limited to:

- reference to security evaluation criteria, methodology and supporting documents used and their version;
- the evaluation technical report;
- the evaluation technical report for composite evaluation (where applicable);
- technical reference documentation;
- developer documentation used in the evaluation effort.

In order to guarantee the reproducibility of the evaluation, all documentation shall be uniquely identified with the proper release date, and proper version number.

40. ANNEX 14: ST SANITISING FOR PUBLICATION

PURPOSE

The Security Target to be included in or referenced by the Certification Report, as requested by Annex 13: CONTENT OF A CERTIFICATION REPORT may be sanitised by the removal or paraphrasing of proprietary technical information. This annex defines the rules for sanitising a Security Target and describes the minimum content of the resulting document which is named ST- lite.

PARTICULAR STATUS

None.

CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE

Annex 13: CONTENT OF A CERTIFICATION REPORT.

1 INTRODUCTION

The Certification Report is the source of detailed security information about the ICT product or protection profile for any interested parties. Its objective is to provide practical information about the ICT product or protection profile to consumers. The Security Target to be included in or referenced by the Certification Report, as requested by Annex 13: CONTENT OF A CERTIFICATION REPORT may be sanitised by the removal or paraphrasing of proprietary technical information. The resulting document is named ST-lite. The ST-lite must be a real representation of the complete ST. This means that the ST-lite cannot omit information which is necessary to understand the security properties of the TOE and the scope of the evaluation.

2 MINIMUM CONTENT

Based on the structural outline of the Common Criteria (CC Part 1, Annex C) the following describes the minimum content of the ST-lite:

- The ST introduction includes in general no proprietary information. Therefore, the introduction need not be sanitized further. The ST-lite needs a unique identifier to be distinct from the complete ST.
- The TOE description might be reduced. It may include proprietary and detailed information about the TOE design which should not be published.
- The TOE security environment description (assumptions, threats, organisational security policies) cannot be reduced. All this information is necessary to understand the scope of the evaluation.
- The security objectives cannot be reduced, all information has to be made public to understand the intention of the ST and TOE evaluation.
- All security requirements have to be made public. Application notes might give information on how CC Part 2 components were used to understand the ST. However, refinements and application notes might be sanitized to remove proprietary information (e.g. about design).
- The TOE summary specification might be sanitized to remove proprietary information (e.g. about design). As a minimum, all TOE Security Functions have to be included.
- The PP claims shall be included.
- The rationale may be sanitized to remove proprietary information.

3 EVALUATION

The TOE evaluation has to be based on a complete Security Target as stated by the criteria.

The ST-lite will not be formally evaluated according to the criteria. The check for the compliance of the ST-lite with the complete Security Target can be performed by the evaluator or the certification body. The Certification Report shall reference both, the complete ST as well as the ST-lite. The CB has to approve the ST-lite for publication.

41. ANNEX 15: PATCH MANAGEMENT

PURPOSE

This annex, for trial use[68], introduces a patch management process in support of the requirements associated to vulnerability handling defined in Chapter 14, RULES RELATED TO HANDLING VULNERABILITIES, and which may also be used for the maintenance activities of certificates, as defined in Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES.

PARTICULAR STATUS

For trial use[69]. The period of the trial use should be of 2 years, but the maintenance organisation of the scheme may propose to reduce this period, be significant progress in its global adoption acknowledged earlier.

CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE

Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES.
Chapter 14, RULES RELATED TO HANDLING VULNERABILITIES.

1 INTRODUCTION

A product may include a patch management mechanism assessed within its certification, under the following conditions. The content of this Annex are supplementing the content of Annex 11, ASSURANCE CONTINUITY. For a certified ICT product, either approaches can be applied, but where the patch management approach has been selected, the following requirements shall apply.

2 APPLICABLE REQUIREMENTS

Such a patch management mechanism may be based:

- on the conditions defined under Patch management ISO SC27 WG3 Technical Report “Extension for Patch Management for 15408 and 18045”, as defined by https://www.jtsec.es/papers/Technical/Report_Patch_Management.pdf;
- or on the ISCI WG1 Proposal for new SAR components and Packages in CC for Patch Management, as defined by https://cclab.com/isci-workgroup.

Applying either of the above, during the initial certification the manufacturer or provider of the ICT product shall:

- detail patching processes following the content and presentation requirements of the accepted patch management process;
- define the TOE boundaries when ADV_ARC is included, and where not, the description of the TOE boundaries shall be put into the Security Target.
- detail Patching mechanisms using the relevant work units of the chosen listed approach.

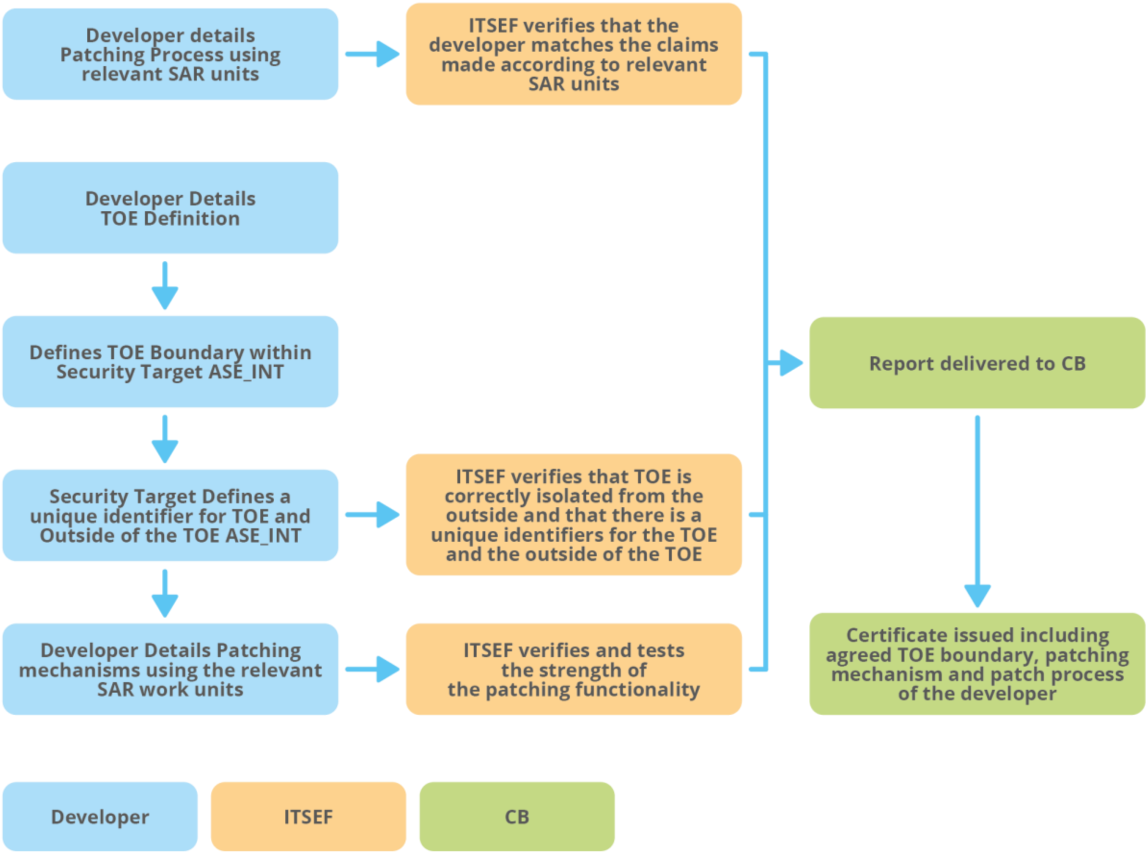
The ITSEF shall verify during the initial certification that the:

- developer implemented the requirements of the accepted patch management process using the relevant SAR work units;
- TOE boundaries are separated in a way that the changes made to the separated processes do not affect the security of the TOE;
- patching mechanisms are working according to the claims made.

[68] As defined in Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS.
[69] As defined in Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS.

The CB shall include in the certification report the applied Patch management mechanism, and shall indicate that it is possible to apply the patch mechanisms described below during the validity of the certificate.

Figure 1: Patch management process



Developer details Patching Process using relevant SAR units

ITSEF verifies that the developer matches the claims made according to relevant SAR units

Developer Details TOE Definition

Defines TOE Boundary within Security Target ASE_INT

Security Target Defines a unique identifier for TOE and Outside of the TOE ASE_INT

ITSEF verifies that TOE is correctly isolated from the outside and that there is a unique identifiers for the TOE and the outside of the TOE

Developer Details Patching mechanisms using the relevant SAR work units

ITSEF verifies and tests the strength of the patching functionality

Report delivered to CB

Certificate issued including agreed TOE boundary, patching mechanism and patch process of the developer

Developer

ITSEF

CB

During the *Remediation development* phase of Vulnerability handling, the eligible patch level shall be determined, based on the elements provided in the vulnerability analysis and in accordance with the following table:

Table 1 : Applicable patch levels

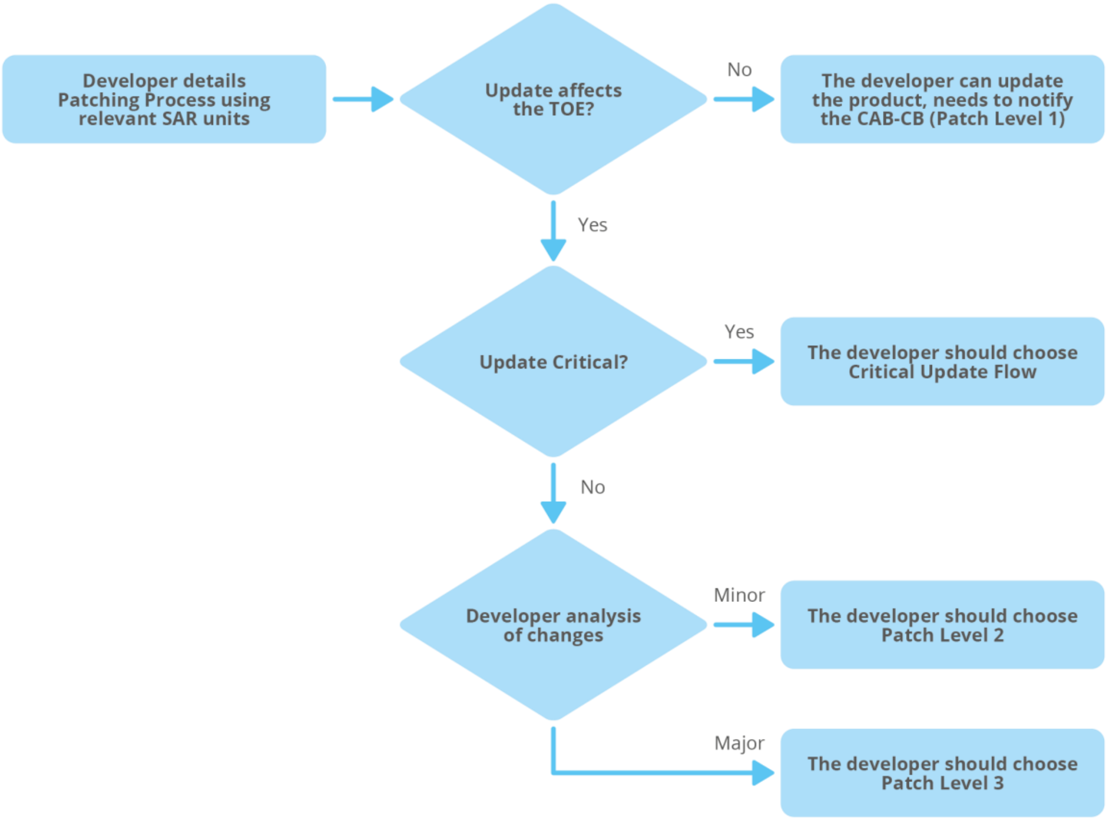
Proximity or availability of the possible attack	Level of change needed to be applied	Patch levels applicable
Attack is available and can be exploited (exploitable vulnerability)	Outside of the TOE	Level 1
	Minor	Critical Update Flow/Level 2
	Major	Critical Update Flow/Level 3
Vulnerability that can be used to develop an attack (exploitable or potential vulnerability)	Outside of the TOE	Level 1
	Minor	Level 2 with potentially Critical Update Flow
	Major	Level 3 with potentially Critical Update Flow
Vulnerability where an attack is not likely or cannot be used for development of an attack potential or residual vulnerability)	Outside of the TOE	Level 1
	Minor	Level 2
	Major	Level 3

The minor/major changes refer to the definitions provided Annex 11, ASSURANCE CONTINUITY, and in the Guidelines for application section below.

The patch levels shall be defined under the following conditions.

Patch Level 1 shall apply where the TOE is part of a bigger ICT product, and product parts not affecting the TOE may be patched whenever required. The initial Common Criteria evaluation shall clearly define the TOE scope and demonstrate that changes outside the TOE scope cannot affect the security of the certified TOE as stated above. The result of this definition and demonstration shall be contained in the Certification Report, detailing what can be changed according to the Patch Level 1 process.

Figure 2: Update Process Developer View


Developer details Patching Process using relevant SAR units
Update affects the TOE?
No
The developer can update the product, needs to notify the CAB-CB (Patch Level 1)
Yes
Update Critical?
Yes
The developer should choose Critical Update Flow
No
Developer analysis of changes
Minor
The developer should choose Patch Level 2
Major
The developer should choose Patch Level 3

Changes to the product under Patch Level 1 shall be made under the decision and the responsibility of the developer. The developer shall inform the CAB within five business days of any such applied changes, and the CAB may decide to apply the maintenance or other relevant CB decision.

Patch Level 2 shall apply for minor changes. For this patch approach to be possible, the applicability to apply a patch shall be evaluated and certified during the initial certification, and the agreed methods shall be applied during the changes.

The manufacturer or provider, after analysis of the applicability of the vulnerability shall develop and test the corrective patch according to the applied accepted approach.

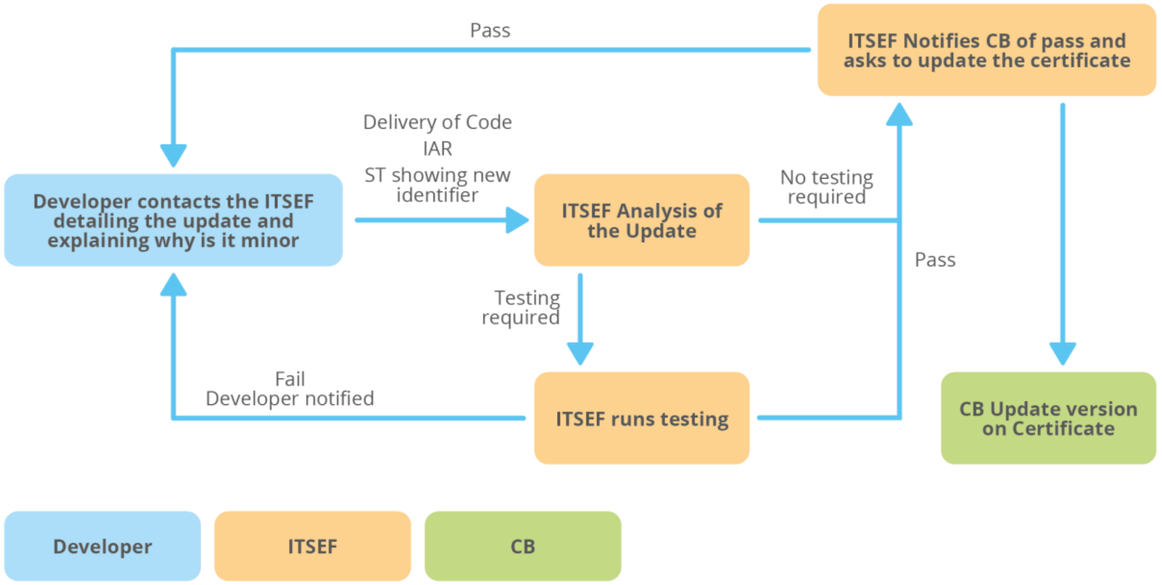
An IAR, together with the changed evidence/documentation shall be established and sent to the ITSEF for its review. In case the changes also affect code, and ADV_IMP is part of the evaluation process, then the code changes shall be reviewed by the ITSEF also. The ITSEF shall proceed to any required testing.

In this Patch Level 2 approach, the ITSEF shall proceed to an evaluation before the product can be patched. A time limit for the evaluation may be agreed between the stakeholders of the process based on the possible damage the exploited vulnerability would present.

The results of the evaluation shall determine whether the patch is declared apt for further deployment or release by the manufacturer or provider.

The ITSEF shall notify the CB of such results and provide the evaluation documentation to both the CB and to the developer. The developer may initiate the patching of the certified ICT product only if the results of the evaluation declared the patch acceptable for release. The patching is the responsibility of the developer of the ICT product. Based on the provided documentation the CB shall decide where applicable to update the version on the certificate, or make a decision based on the certification process. The patch application does not have to wait here for the results of the certification process.

Figure 3: Patch Level 2


Pass
ITSEF Notifies CB of pass and asks to update the certificate
Delivery of Code
IAR
ST showing new identifier
Developer contacts the ITSEF detailing the update and explaining why is it minor
ITSEF Analysis of the Update
No testing required
Pass
Testing required
Fail
Developer notified
ITSEF runs testing
CB Update version on Certificate
Developer
ITSEF
CB

Patch Level 3 shall consist of the application of the already existing provisions defined by Annex 11, ASSURANCE CONTINUITY, for a major change.

Critical Update Flow process: this additional patch level shall apply for changes where an attack is already possible to be exploited or update is critical and needs to be released urgently. Intended use cases may include:

- Vulnerabilities that are publicly known and exploitable;
- The Product is used within critical infrastructure;
- Liability issues are applicable;
- Safety is at risk.

Critical Update Flow process shall not replace Patch Level 2 or 3, and shall be used as a way for the manufacturer or provider to deploy or release a critical update quickly and then follow Patch Level 2 or 3 at a later date.

Crititical update flow can only be applied to TOEs, where the relevant patch mechanisms have been certified. The application of the critical update flow is the responsibility of the manufacturer or provider of the ICT Product.

The manufacturer or provider, after verification of the applicability of the vulnerability and assessment that this patch is of critical nature, shall develop and test the corrective patch according to the applied accepted approach.

This is the only case where the patch is deployed or released prior to review. The ITSEF and the CB shall be informed within five business days of the changes, and shall perform the necessary evaluation and certification activities. This process may start in parallel with the change but the patch application does not have to wait for the results of the evaluation and certification process.

The ITSEF shall evaluate the already deployed patch with the highest priority, in order to evaluate the changes and create the relevant documentation in previously agreed time according to the agreement made with the manufacturer or provider. The evaluation results shall be sent to the CB.

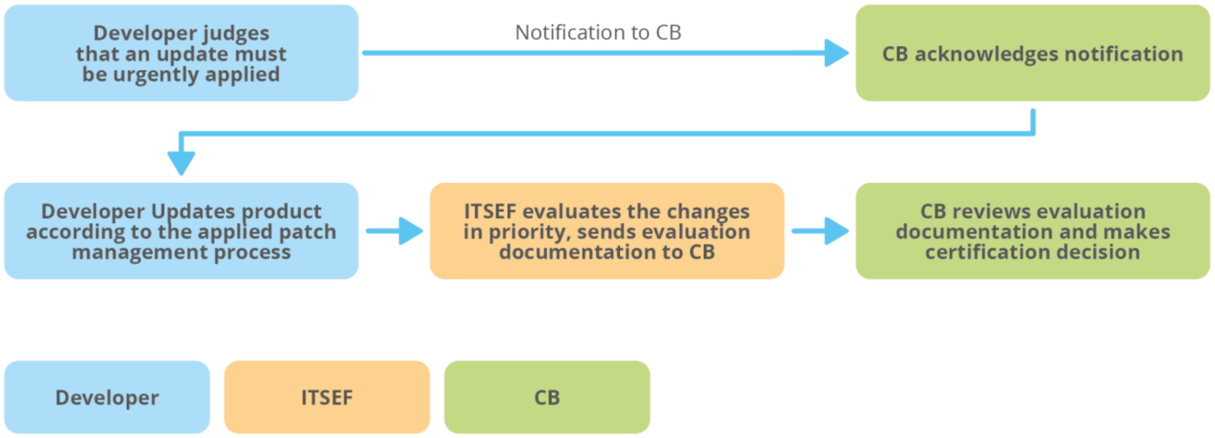
Based on the provided documentation the CB shall decide where applicable to update the version on the certificate, or make a decision based on the certification process.

The avaibility of a patch shall be communicated through the means defined by the manufacturer or provider of the ICT product, described in the guidance according to CSA Article 55. The users of the ICT product shall be included amongst the receivers of information about a possibility of a patch to a certified TOE, which the manufacturer or provider of the

ICT product intends to include in the scope of the certificate. In all cases, where the patch mechanism has been successfully applied, a new certificate shall be issued, which validity period shall not exceed the validity of the original certified ICT product.

Note: The patch management system may as well be used by a manufacturer or provider for functional patches of its ICT product. This shall only apply under the condition that the approach Patch Level 1 is used, or that it is bundled with vulnerability patches and do not affect TSFIs neither directly nor indirectly, and also do not change the security functionalities satisfying the security functional requirements.

Figure 4: Critical Update Flow


Developer judges that an update must be urgently applied
Notification to CB
CB acknowledges notification
Developer Updates product according to the applied patch management process
ITSEF evaluates the changes in priority, sends evaluation documentation to CB
CB reviews evaluation documentation and makes certification decision
Developer
ITSEF
CB

3 GUIDELINES FOR APPLICATION

Table 2: Applicable actions of the patch levels

Actions/Patch levels	Action 1	Action 2	Action 3	Comment
Patch level 1	Changes to the product under Patch Level 1 shall be made under the decision of the Manufacturer.	The Manufacturer shall inform the CAB within five business days of any such applied changes.	The CAB may decide to apply the maintenance or other relevant CB decision.	
Patch level 2	Manufacturer develops and tests the corrective patch according to the applied accepted approach. (No required time limit set).	ITSEF shall proceed to an evaluation before the product can be patched. This is documented by the ITSEF. A time limit for the evaluation may be agreed between the stakeholders of the process.	If the evaluation result allows it, the Manufacturer can patch the product.	Based on the provided documentation the CB shall decide where applicable to update the version on the certificate, or make a decision based on the certification process.
Patch level 3	Annex 11, ASSURANCE CONTINUITY, for a major change.			
Critical Update Flow	Manufacturer/Provider develops corrective patch (No time limit set).	The ITSEF and the CB shall be informed of the changes within five business days, and shall perform the necessary evaluation and certification activities. The patch application does not have to wait for the results of the certification process.	The ITSEF shall evaluate the already deployed patch with the highest priority, in order to evaluate the changes and create the relevant documentation in previously agreed time, according to the agreement made with the manufacturer or provider.	Based on the provided documentation the CB shall decide where applicable to update the version on the certificate, or make a decision based on the certification process.

The patch management approach of the EUCC scheme may only be applied if the ICT product conforms to the relevant requirements during its initial certification. These include the ISCI WG1 “Proposal for new SAR components and Packages in CC for Patch Management” and the Patch management ISO SC27 WG3 Technical Report “Extension for Patch Management for 15408 and 18045”. When the ICT Product does not comply with one of these, then the Assurance continuity requirements defined in Annex 11 shall apply.

The two (2) accepted processes both aim for an assurance of the patch development and deployment process.

The ISCI WG1 Proposal for new SAR components and Packages in CC for Patch Management intends to apply an asynchronous evaluation and certification process assuming trust in the already evaluated patch development and deployment, and provides the necessary SARs and work units.

The ISO SC27 WG3 Technical Report “Extension for Patch Management for 15408 and 18045” defines building blocks (i.e. SFRs for patch functionality and one additional ALC family) which can be integrated into PPs and STs to provide additional assurance for the TOE’s patching functionality and the developer’s patch management process.

Note that both approaches provide the necessary assurance to handle the issues of updating certified products and may be either chosen for application, in their latest applicable version. The ISCI WG1 proposal has been set up to be used for the Smart cards and similar devices technical domain. The ISO Technical Report is a more general approach. Both can be applied to all products aiming to reach substantial and high level of assurance. Both approaches are still subject to further improvements.

There are four (4) acceptable levels of patch management; 1,2,3 and Critical Update Flow.

The Patch management approach of the EUCC scheme starts with the discovery of a previously undetected cybersecurity vulnerability related to the certified ICT product.

The second step is the acknowledgement that the manufacturer or provider will analyse the product and provide a date to the CB for when they will reply with analysis describing whether the vulnerability applies to the product. When the vulnerability is disproved, the related documentation needs to be kept, but the process ends. The analysis shall also contain verification by the ITSEF and the CB about the Attack potential calculation, taking into consideration also whether the previously calculated attack potential of a vulnerability changed since.

When the vulnerability applies to the certified ICT product, the next step is the triage to weigh the possible risks and eligible patch levels.

The triage process takes into account the following measures:

1. proximity or availability of the possible attack;
2. level of the change that the manufacturer or provider needs to apply for patch management process. The changes of minor and major are the levels defined in the JIL AC process.

The minor/major levels of changes may be further refined with examples during the initial certification to speed up the decision-making process, but this refinement shall adhere to the definitions of Annex 11, ASSURANCE CONTINUITY.

There are two (2) additions to Assurance continuity in the EUCC patch management approach:

1. bug-fixes are considered typical minor changes here;
2. changes to the ICT environment that do not change the certified TOE are considered to be applicable at Patch Level 1.

The list should be expanded by the expert groups in charge of the maintenance of the EUCC scheme.

The manufacturer or provider should document the details of the changes and the possible effects of application/not application of the patches, and send this document to the users of the product as well as the ITSEF and CB. This way the users of the certificate can also assess the possible risks based on the data provided by the manufacturers or providers. It may be of good practice to also document the risk assessment to the users, ITSEF and CB.

The manufacturer shall reach an agreement with the CB and ITSEF about the conditions of the future patch management processes. Also, it shall be noted that whatever the path indicated by the analysis, the developer may for any reason not patch the product. The table identifies the possible applicable process for each case, but doing nothing is always a possibility (that has consequences on the impacted certificate(s) as provided in Chapter 13).

The asynchronous approach, which can be described as the possibility that the security analysis of the correction is assessed by the ITSEF and CAB after the patch has been applied or released, is to be accepted only for the Critical Update Flow Process. For the other levels, the following is applied:

- in Patch Level 1 the CB is notified and able to apply maintenance process if deemed necessary;
- in Patch Level 2 the ITSEF evaluates synchronously and CB is again notified and can decide whether to update the version on the certificate;
- in Patch Level 3 the process is fully synchronous.

A future update of the EUCC scheme may consider applying more widely the asynchronous approach.

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu