

COMMON CRITERIA FOR SOFTWARE AND EMBEDDED PRODUCTS

Implementation Guide

SECURA

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)88 888 3100
E info@secura.com
W secura.com

Follow us on   



1. What is Common Criteria?

1.1 Introduction to Common Criteria

The **Common Criteria for Information Technology Security Evaluation**, shortly referred to as **Common Criteria or CC**, is an international standard for independent security evaluation and certification of IT products implemented as hardware, firmware or software.

Common Criteria consists of three main parts plus the recommended methodology to perform evaluations:

- **Part 1:** Introduction and general model, April 2017, version 3.1, revision 5 [1];
- **Part 2:** Security functional components, April 2017, version 3.1, revision 5 [2];
- **Part 3:** Security assurance components, April 2017, version 3.1, revision 5 [3];
- Common Methodology for Information Technology Security Evaluation (further referred to as CEM), April 2017, version 3.1, revision 5 [4].

The global benefits of CC certification include:

- Guarantee that the process of certification of IT products was conducted in a transparent and standardized manner;
- Guarantee of the acceptance and mutual recognition of the certificates for IT products on international level;
- Increase in the amount of certified products with assured security available for IT professionals.

There are **three main categories of IT products** commonly certified based on CC requirements:

- General types of IT products;
- Smartcards and similar devices,
- Hardware Device with Security Boxes.

Table of Contents

1. What is Common Criteria?	3
2. Common Criteria Requirements	5
3. Common Criteria Certification	
Overview & Examples	7
4. Harmonization of Common Criteria	
under the EU Cybersecurity Act	17
5. Further Clarifications	18
Interested in Common Criteria?	21
Appendix A. List of References	22
Appendix B. Abbreviations	23

1.2. Key concepts of Common Criteria

Several important concepts are introduced within Common Criteria which are essential for the understanding of the certification process, as presented below.

- **Target of Evaluation (TOE).** Set of software, firmware and/or hardware possibly accompanied by guidance that is evaluated based on CC requirements. Represents the evaluated IT product or its part(s).
- **Protection Profile (PP).** A document containing implementation-independent statement of security needs for a specific TOE type in form of requirements
- **Security Target (ST).** A document containing implementation-dependent statement of security needs for a specific identified TOE in form of requirements. The ST can claim conformance to a particular PP in case of a specific type of TOE.
- **Security Functional Requirements (SFRs).** Security requirements that are presented for individual security functions of TOE.
- **Security Assurance Requirements (SARs).** Security requirements that are used to represent the activities performed during the conducted evaluation, to provide a certain level of assurance in the security of TOE.
- **Sponsor of the evaluation.** The party that plans to certify TOE (could be either a developer of the product or a third party).
- **National certification scheme.** National CC scheme, providing own set of tailored rules for evaluation and certification of IT products, based on the CC standard [1] – [4].
- **IT Security Evaluation Facility (ITSEF).** Accredited and licensed lab, specialized in performing CC evaluations for a particular class of IT products
- **Package.** A named set of either security functional or security assurance requirements.
- **Evaluation Assurance Level (EAL).** Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package.

1.3. National schemes for Common Criteria and mutual recognition of issued certificates

The national schemes which can either issue or accept CC certificates are grouped worldwide under the CCRA (Common Criteria Recognition Agreement). This mutual recognition agreement ensures the international recognition of issued CC certificates up to evaluation level EAL2.

Additionally, the mutual recognition of the certificates between different countries in Europe is ensured by SOG-IS (Senior Officials Group Information Systems Security) “Mutual Recognition Agreement of Information Technology Security Certificates” signed in January 2010 [7]. Participants in this Agreement are government organisations or government agencies from countries of the European Union or EFTA (European Free Trade Association), representing their country or countries. Within SOG-IS, the issued CC certificates are mutually recognized up to the level at which they were released. In other words, an EAL4 certificate issued in a country member of SOG-IS will be directly recognized as EAL4 in any other SOG-IS country.

In the Netherlands, the certification based on Common Criteria is performed under the “**Netherlands Scheme for Certification in the Area of IT Security**” (NSCIB). The Netherlands National Communications Security Agency (NLNCSA), Ministry of the Interior and Kingdom Relations is the responsible national body in the Netherlands for Common Criteria evaluations.

This document will further focus on the NSCIB procedures for particular evaluation activities and processes. More on the processes of working with NSCIB scheme is presented in section 3.1.



2. Common Criteria Requirements

Common Criteria introduces two types of requirements:

- **Security Functional Requirements** (SFRs) presented in CC Part 2: Security functional components;
- **Security Assurance Requirements** (SARs) presented in CC Part 3: Security assurance components.

Every IT product aimed at certification according to CC requirements should claim a set of requirements that they comply with. The claim should be presented in a form of a document which is called a Security Target (ST). According to Common Criteria, the following information should be included in the Security Target (see table below).

Creating the Security Target is an important process in obtaining the certification for the product, since all the following evaluation activities are based on it. The creation of the Security Target is the responsibility of the sponsoring party who would like to certify the product (it might be either the developer of the product or a third party). It might happen that the sponsor of the evaluation does not have the necessary expertise or experience to create a Security Target themselves. In this case, it is highly recommended to use a support of the consultants from evaluation laboratories to create the Security Target. This will allow for additional assurance of the smooth certification process.

The concept of packages is introduced by Common Criteria to simplify the process of selection of requirements for the product. An example of a package is EAL3.

- **Depth of evaluation** - the effort is greater because it is deployed to a finer level of design and implementation detail;
- **Coverage of evaluation** – the effort is greater because more evaluation requirements are in scope
- **Rigour of evaluation**, the effort is greater because it is applied in a more structured, formal manner.

The assurance increases with every level, the “default” levels in a CC evaluation are identified in the following way:

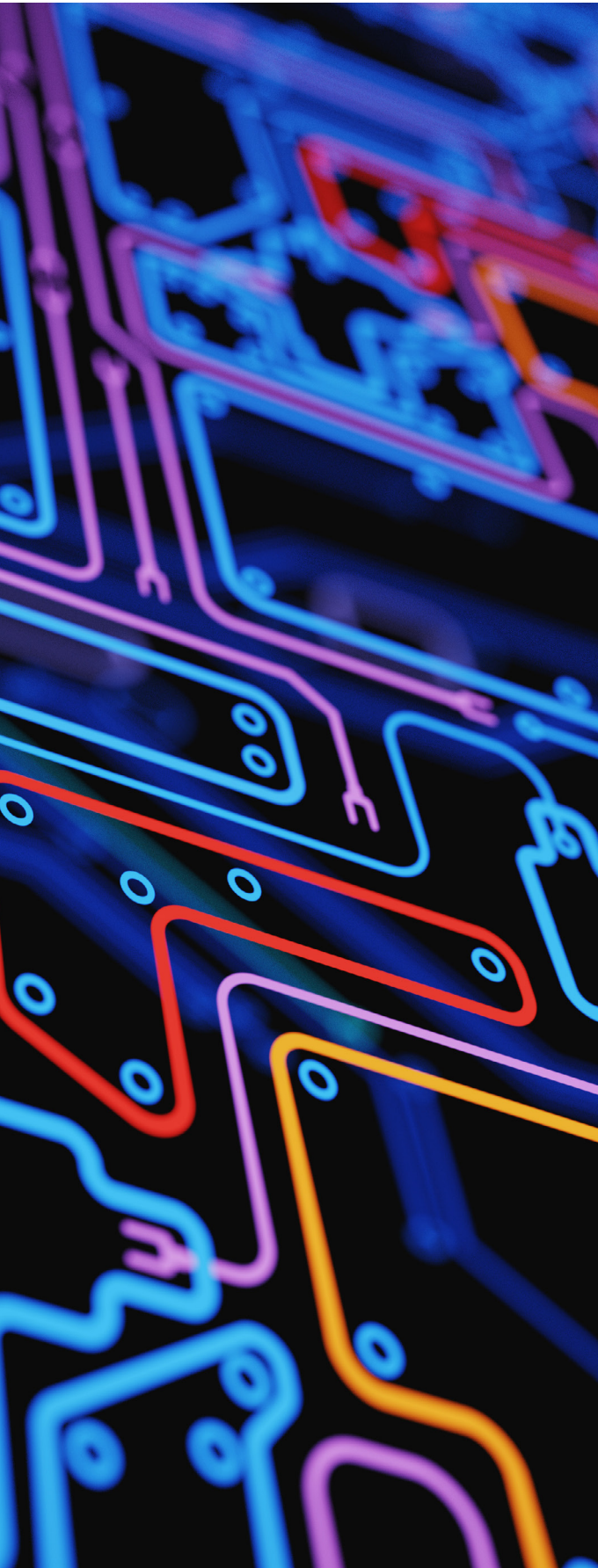
- **EAL1** – functionally tested;
- **EAL2** – structurally tested;
- **EAL3** – methodically tested and checked;
- **EAL4** – methodically designed, tested and reviewed;
- **EAL5** – semi-formally designed and tested;
- **EAL6** – semi-formally verified design and tested;
- **EAL7** – formally verified design and tested.

For every evaluation level, different assurance requirements are applicable. Every requirement represents a single activity that should be performed on the product and related processes (assurance component).

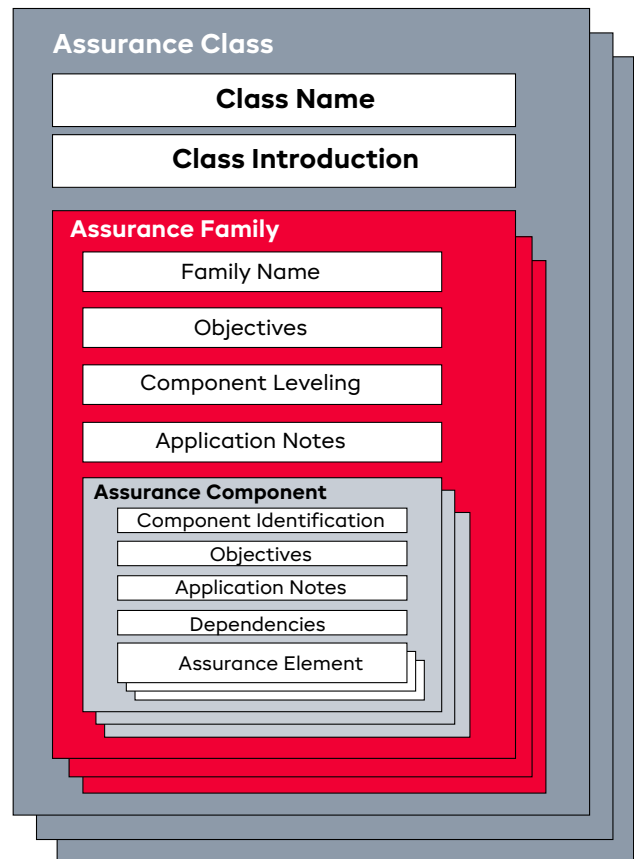
Content	Description	Remarks
Product Overview	Description of the typical functionality of the product including the description of typical usage and scope of the evaluation.	-
Security Problem Definition	Description of threats that the product addresses, security policies that it should adhere to, assumptions about the product environment to ensure the proper functioning of the product, security objectives that should be satisfied by the product.	All security objectives should be mapped to threats, security policies and assumptions.
Security Functional Requirements	A set of security requirements that the product aims to achieve, extracted from CC Part 2 ¹ .	Every SFRs should be mapped to previously identified objective of the product
Security Assurance Requirements	A set of assurance requirements based on which the product will be evaluated, extracted from CC Part 3 ² .	In accordance with a desired level of assurance (EAL).
Security Functions	A summary of security functions provided by the product.	All security functions should be mapped to the SFRs identified previously

¹ If certain features of the product cannot be expressed using existing SFRs, additional SFR might be created within Security Target. In this case, the conformance to CC Part 2 extended should be claimed in Security Target.

² If additional SARs are required to express the desired level of assurance, they might be included in the Security Target. In this case the EAL would be stated as EAL augmented.



The requirements are grouped based on the topics of evaluation and form different families and classes. **The structure of a typical assurance class is presented below.**



Another important concept introduced by Common Criteria is the concept of **Protection Profiles**. A Protection Profile is a document created by different user communities that identifies security requirements for a specific class of security devices (for example, firewalls). Sponsors of the evaluation can choose to implement products that comply with one or several Protection Profiles and have their products evaluated against them. This makes Protection Profiles possible alternatives to CC evaluations conducted against a pre-defined EAL level. Protection Profile based evaluations are especially attractive when the target product fits fully within a well-established product category, for example payment devices or routers. In this case, an already existing Protection Profile can be directly used in order to define the relevant threats and security requirements for the product.

Every Protection Profile needs to be certified separately before it can be used as a basis for evaluation. Moreover, its suitability needs to be confirmed with the certification scheme before the start of the evaluation.

3. Common Criteria Certification Overview and Examples

3.1. Certification process and main stakeholders

The certification process according to NSCIB procedures [5] includes three main phases:

- **Phase 1: Preparation** in which the formal Application shall be submitted and processed, resulting in a signed Certification Agreement and an approved Evaluation Work Plan.
- **Phase 2: Evaluation review** (monitoring) in which the evaluation activities are performed under supervision of the Certification Body (CB), resulting in an Evaluation Technical Report (ETR) as well as other required intermediate deliverables.
- **Phase 3: Certification** in which the concluding actions are performed, resulting in a Certificate for the evaluated product.

The diagram showing the whole certification process according to NSCIB certification procedures [5] is presented on the below.

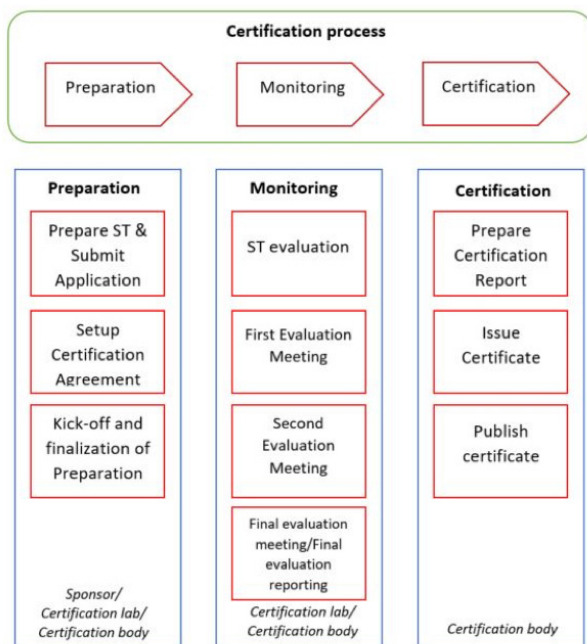


Figure 1 - NSCIB certification process

The following main parties are involved in the certification process under NSCIB:

- **Certificate Issuer** – TÜV Rheinland NL
- **Support Certification Body** – TrustCB.
- **Certification Monitor** – NLNCSA.
- **Evaluation Laboratory** – ITSEF (a licenced laboratory that performs evaluation activities, for example, Secura)
- **TOE Developer** – Company developing (and/or manufacturing) the TOE used for the CC evaluation
- **Evaluation Sponsor** – Third party sponsoring the CC evaluation process. The Sponsor is often the same entity as the Developer

3.2. Example evaluation procedure for a software product for EAL3

To provide a better understanding of the evaluation procedures (Monitoring phase in the certification process) we will take as an example the evaluation of a general software product evaluated under EAL3 requirements.

Applicable classes of SARs for EAL3 include:

- Security Target evaluation (ASE);
- Development documentation (ADV);
- Guidance documentation (AGD);
- Life-cycle support (ALC);
- Tests applicable to the product (ATE);
- Vulnerability assessment for the product (AVA).

The description for each class of activities is presented further.

Based on the results of evaluation for every activity, certain updates might be needed to satisfy particular CC requirements in the developer's processes, documentation or the TOE itself. Implementing those changes is the responsibility of the developer of the TOE³.

³ As an additional service, an evaluation laboratory can provide consultancy services for the developer to support him in implementing the required changes.



3.2.1. ASE Activities

Typically, under NSCIB, the evaluation process starts with the evaluation of the TOE's Security Target. The evaluation of the Security Target is aimed to demonstrate that the Security Target is internally consistent, follows the applicable CC requirements and presents the correct claim to packages and PPs (when applicable).

The following assurance families are included in an EAL3 evaluation for ASE class (see below).

To perform the ASE evaluation activities, the following input from the developer is required:

- **Security Target** for evaluated product.

During the evaluation, the provided Security Target is analysed to determine whether all applicable requirements of ASE families are met. Results of the ST evaluation are presented in a separate report for ASE activities (called IR_ASE).

Assurance Family	Objective
ASE_CCL.1	Determine the validity of the conformance claim.
ASE_ECD.1	Determine that (any) extended components are clear and unambiguous, and that they are necessary.
ASE_INT.1	Demonstrate that the ST and the TOE are correctly identified, that the TOE is correctly described at three levels of abstraction and that these three descriptions are consistent with each other.
ASE_OBJ.2	Demonstrate that the security objectives adequately and completely address the security problem definition, that the division of this problem between the TOE and its operational environment is clearly defined.
ASE_REQ.2	Ensure that security requirements are clear, unambiguous and well-defined.
ASE_SPD.1	Demonstrate that the security problem intended to be addressed by the TOE and its operational environment is clearly defined.
ASE_TSS.1	Determine whether TOE summary adequately describes how the TOE meets its SFRs, protects itself against interference, logical tampering and bypass and whether the TOE summary specification is consistent with other narrative descriptions of the TOE.

3.2.2. ADV Activities

The following assurance families are included in an EAL3 evaluation for ADV class:

Assurance Family	Objective
ADV_ARC.1	The objective of this family is for the developer to provide a description of the security architecture of the TOE Security Functionality (TSF). The TSF can be the whole product, or a subset of the product. This will allow analysis of the information that, when coupled with the other evidence presented, will confirm the TSF achieves the desired properties. The security architecture description supports the implicit claim that security analysis of the TOE can be achieved by examining the TSF.
ADV_FSP.3	This family levies requirements upon the functional specification, which describes the TSF interfaces (TSFIs). The TSFI consists of all means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF. This family provides assurance directly by allowing the evaluator to understand how the TSF meets the claimed SFRs.
ADV_TDS.2	This family aims to confirm that the product is clearly described in its development documentation in terms of subsystems, including particular components and functionalities offered by these subsystems and the interaction between them. The mapping between the defined subsystems and the claimed SFRs is also investigated.

To perform the **ADV evaluation activities**, the following input from the developer is required:

- **Architectural description of the TOE** including description for all security features, subsystems and interfaces. This can be provided in a single document or extracted from different documents.

The evaluator analyses the provided architectural description to determine whether all applicable requirements of ADV families are met. Additional information might be obtained through meetings organized with the product's developer.

As the result of this activity the evaluator should have a complete understanding of the TOE (including subsystems and modules), its security functions and security architecture and all available interfaces.

The main results of the ADV activities are recorded in a form of an ADV Presentation and should be presented by the evaluator during Evaluation Meeting 1 (EM1). Additionally, summary of verdicts for ADV activities are recorded in a reference document for ADV and AGD activities, see section

3.2.3. AGD Activities

The following assurance families are included in an EAL3 evaluation for AGD class (see table below).

Assurance Family	Objective
AGD_OPE.1	Operational user guidance refers to written material that is intended to be used by all types of users of the TOE in its evaluated configuration: end users, persons responsible for maintaining and administering the TOE in a correct manner for maximum security, and by others (e.g. programmers) using the TOE's external interfaces. Operational user guidance describes the security functionality provided by the TSF, provides instructions and guidelines (including warnings), helps to understand the TSF and includes the security-critical information, and the security-critical actions required, for its secure use. The operational user guidance provides a measure of confidence that non-malicious users, administrators, application providers and others exercising the external interfaces of the TOE will understand the secure operation of the TOE and will use it as intended.
AGD_PRE.1	Preparative procedures are useful for ensuring that the TOE has been received and installed in a secure manner as intended by the developer. The requirements for preparation call for a secure transition from the delivered TOE to its initial operational environment. This includes investigating whether the TOE can be configured or installed in a manner that is insecure but that the user of the TOE would reasonably believe to be secure.

To perform **the AGD evaluation activities** the following input from the developer is required:

- User manuals for the product;
- Administrator guidance including description of secure delivery procedures and installation of the product⁴.

The evaluator analyses the provided manuals to determine whether all applicable requirements of AGD families are met. Results of the AGD activities are recorded in a reference document (ADV/AGD Reference document) together with the summary of ADV verdicts and are presented by the evaluator at EM1.

3.2.4. ALC Activities

The following assurance families are included in an EAL3 evaluation for ALC class (see table below).

To perform the ALC evaluation activities the following input from the developer is required:

- Configuration Management Plan including the list of configuration items related to the product;
- Development confidentiality and integrity policies including description of all physical, procedural, personnel and other security measures which ensure the preservation of the product's confidentiality and integrity during development;
- Description of product delivery procedures (might be part of User or Administrator Manuals);
- Product life-cycle documentation including the description of the used life-cycle model.

Assurance Family	Objective
ALC_CMC.3	Configuration management (CM) is one means for increasing assurance that the TOE meets the SFRs. CM establishes this by requiring discipline and control in the processes of refinement and modification of the TOE and the related information. CM systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking any changes, and by ensuring that all changes are authorised. The objective of this family is to require the developer's CM system to have certain capabilities. These are meant to reduce the likelihood that accidental or unauthorised modifications of the configuration items will occur. The CM system should ensure the integrity of the TOE from the early design stages through all subsequent maintenance efforts.
ALC_CMS.3	The objective of this family is to identify items to be included as configuration items and hence placed under the CM requirements of CM capabilities. Applying configuration management to these additional items provides additional assurance that the integrity of TOE is maintained.
ALC_DEL.1	The concern of this family is the secure transfer of the finished TOE from the development environment into the responsibility of the user. The requirements for delivery call for system control and distribution facilities and procedures that detail the measures necessary to provide assurance that the security of the TOE is maintained during distribution of the TOE to the user. For a valid distribution of the TOE, the procedures used for the distribution of the TOE address the objectives identified in the PP/ST relating to the security of the TOE during delivery.
ALC_DVS.1	Development security is concerned with physical, procedural, personnel, and other security measures that may be used in the development environment to protect the TOE and its parts. It includes the physical security of the development location and any procedures used to select development staff.
ALC_LCD.1	Poorly controlled development and maintenance of the TOE can result in a TOE that does not meet all of its SFRs. Therefore, it is important that a model for the development and maintenance of a TOE to be established as early as possible in the TOE's life-cycle. Using a life-cycle model that has been approved by a group of experts (e.g. academic experts, standards bodies) improves the chances that the development and maintenance models will contribute to the TOE meeting its SFRs. The use of a life-cycle model including some quantitative valuation adds further assurance in the overall quality of the TOE development process.

⁴ User and Administrator guidance can be presented within the single document.

The ALC evaluation activities are performed in three steps:

1. Identifying the configuration items of the TOE and their versioning system. The detailed results are recorded in ALC Configuration Presentation and presented by an evaluator at EM1.
2. Analysing the existing change management system, life-cycle model and security measures that are implemented in the development process of the TOE. The detailed results are recorded in ALC Presentation and presented by an evaluator at EM2.
3. Analysing the presented evidence that the change management system and security measures are implemented accordingly to documentation. The results are recorded in ALC Evidence Presentation and presented by an evaluator at EM3.

3.2.5. ATE Activities

The following assurance families are included in an EAL3 evaluation for ATE class.

To perform the ATE evaluation activities the following input from the developer is required:

- Test plans and test results including testing results of all subsystems, modules and interfaces and triggering all possible error messages.

The evaluation of ATE activities are performed in three steps:

1. Evaluating the developer's test results. The results are recorded in ATE/AVA Presentation which is presented to the scheme during EM2.
2. Creating evaluator's ATE test plans (combined with AVA test plans, see section 3.2.6). The detailed ATE test plans are recorded in ATE/AVA Test Descriptions and presented to the scheme during EM2.
3. Performing ATE tests. The testing results are recorded in ATE/AVA Test Results Presentation and presented to the scheme during EM3.

For ATE testing (step 3 above) the following test approach is implemented:

- Several developer tests are repeated;
- Additional tests developed by the evaluator are performed based on the created test plan.

The repeated tests are commonly selected based on the following criteria:

- Criticality of the tests;
- Depth of provided test evidence.

Assurance Family	Objective
ATE_COV.2	This family establishes that the TSF has been tested against its functional specification. This is achieved through an examination of developer evidence of correspondence.
ATE_DPT.2	The components in this family deal with the level of detail to which the TSF is tested by the developer. Testing of the TSF is based upon increasing depth of information derived from additional design representations and descriptions. The objective is to counter the risk of missing an error in the development of the TOE. Testing that exercises specific internal interfaces can provide assurance not only that the TSF exhibits the desired external security behaviour, but also that this behaviour stems from correctly operating internal functionality.
ATE_FUN.1	Functional testing performed by the developer provides assurance that the tests in the test documentation are performed and documented correctly. The correspondence of these tests to the design descriptions of the TSF is achieved through the Coverage (ATE_COV) and Depth (ATE_DPT) families. ATE_FUN contributes to providing assurance that the likelihood of undiscovered flaws is relatively small.
ATE_IND.2	The objectives of this family are built upon the assurances achieved in the ATE_FUN, ATE_COV, and ATE_DPT families by verifying the developer testing and performing additional tests by the evaluator.

3.2.6. AVA Activities

The following assurance families are included in an EAL3 evaluation for AVA class.

Assurance Family	Objective
AVA_VAN.2	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.

No documentation input from the developer is required for performing AVA activities. However, the TOE needs to be fully available for testing, in an environment that is equivalent with the one described in the TOE's Security Target.

The evaluation of AVA activities is typically performed in two steps:

1. Creating the evaluator's AVA test plans (combined with ATE test plan as described previously). The detailed AVA test plans are recorded in ATE/AVA Test Descriptions and to the scheme during EM2.
2. Performing AVA tests. The testing results are recorded in ATE/AVA Test Results Presentation and presented to the scheme during EM3.

AVA testing is performed in the following steps:

- Analysis of publicly known vulnerabilities;
- Attempting to exploit identified applicable publicly known vulnerabilities;
- Performing additional independent testing based on the developed test plan.

The types of tools used during the conducted testing depend strongly on the type of the product and the identified attack scenarios. For the purpose of exemplification, given the considered software-type product, following tools for software application testing are commonly used, such as:

- Basic Ubuntu system utilities: grep, strings, awk, base64, curl, tar, openssl, nc, etc.
- Network assessment tools: Wireshark, nmap, etc.
- Web application assessment tools: Burp Suite Pro, SQLmap, etc.
- Vulnerability scanners: Nessus, OpenVAS, etc.
- Reverse engineering tools.



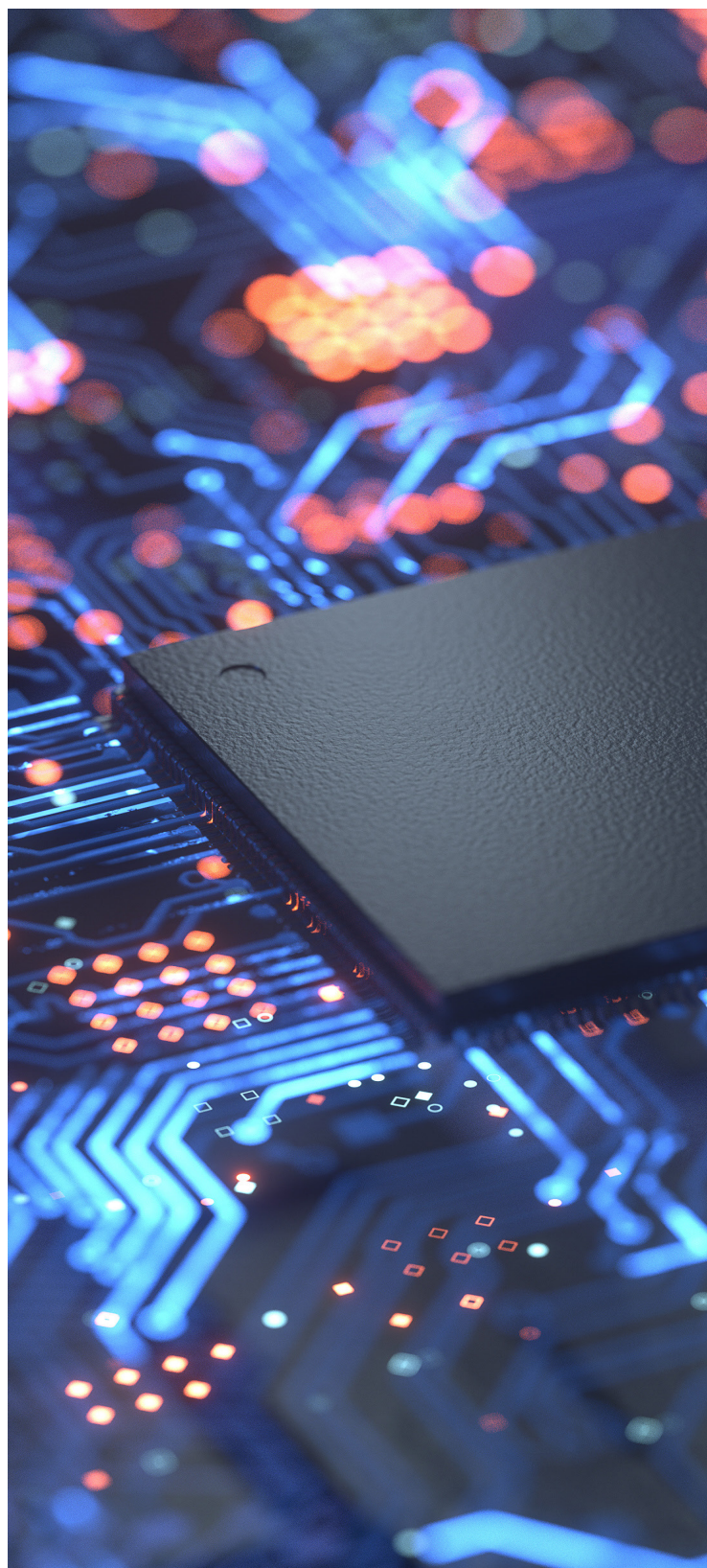
3.3. What to expect from an EAL3 evaluation of an embedded product (e.g. IoT, ICS, medical device)?

Embedded products can be smoothly evaluated and certified under a Common Criteria scheme. In principle, the process presented in detail in section 3.2 applies also in case when an embedded product is the TOE. Examples of embedded products which can be evaluated under CC include smart consumer products (cameras, smart lights, home appliances, etc.), ICS components and systems, medical devices, smart meters, connected printers, and more.

The only main difference which could be expected in the evaluation process deals with the scope of testing. When an embedded product represents the TOE, the selection of relevant tests to include in the test plan will focus on possible vulnerabilities applicable to these types of products.

Examples of such testing could include fuzzing, side channel analysis, malicious software updates, authentication and authorization controls validation, security of data in transit and at rest, security of implemented protocols (e.g. Bluetooth, Wi-Fi, TLS, etc.). In line with such attack vectors, the list of relevant applicable tooling will also be slightly different than in the case of software products, this time including tools such as protocol analysers, fuzzing tools, chip programmers, code analysers, DoS attack tools, interfaces and ports scanners, vulnerability scanners, etc.

The effort associated with the evaluation of an embedded device should in principle not deviate considerably from the one considered for a software product, however it depends on several factors. On one hand, the effort is strongly linked with the scope and complexity of the TOE. More external interfaces, more offered security functionalities or simply more components of the TOE in scope will translate in more time needed for the architecture review and vulnerability assessment. At the same time, other classes of evaluation (for example ASE, AGD, ALC and ATE) should not be strongly impacted by the scope difference or by the type of TOE considered.



3.4. What to expect from other evaluation levels?

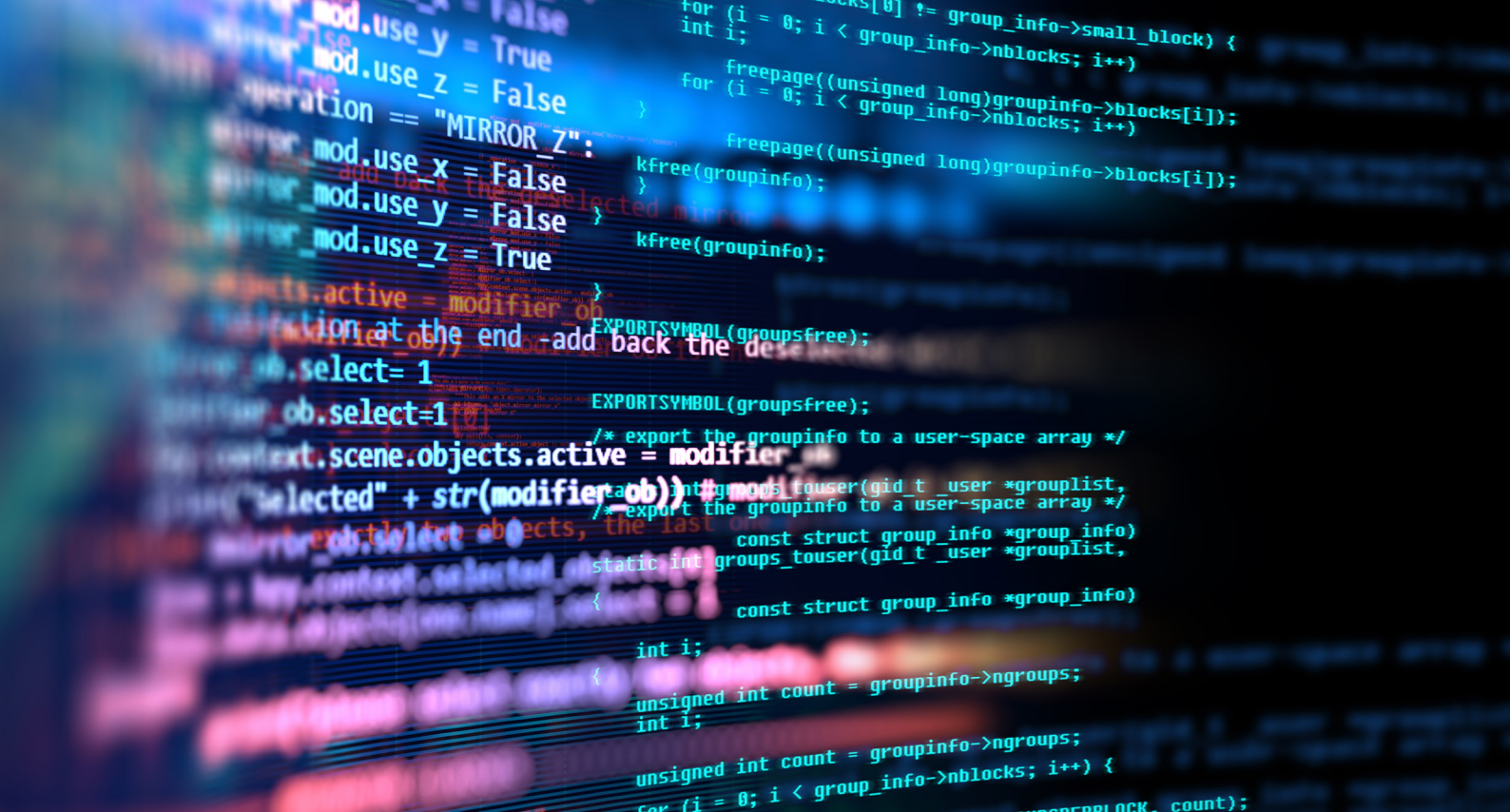
Sections 3.2 and 3.3 described the typical CC evaluation process for an **EAL3 evaluation**. But what to expect from lower or higher levels of evaluation? In Common Criteria, the coverage and depth of the evaluation activities increases the higher selected EAL gets. This means that an **EAL1 evaluation** will have the lowest associated volume and depth of evaluation activities. Below some examples will be given concerning differences between levels 1, 2, 3 and 4 of a CC evaluation.

An **EAL1 evaluation** is the base level of Common Criteria. This level will contain the minimal coverage in terms of TOE architecture analysis (ADV part), which is limited to the assessment of the product's security relevant interfaces. The development processes (ALC part) are also minimized, with focus solely on the configuration management systems implemented by the developer. From a testing point of view (ATE class), the EAL1 level asks for the ITSEF to conduct independent testing on a subset of the TOE, without the need to additionally inspect the developer's own test results. Still a vulnerability analysis activity (AVA) is required, focused at concluding that the product is resistant to basic attack scenarios. Finally, Security Target (ASE) and user guidance (AGD) evaluation activities are required.

For an **EAL2 evaluation**, more emphasis is put on the products development architecture, which needs to include sufficient argumentation on how the product initializes and protects itself against attacks. On the processes side, additionally the product delivery procedures need to be inspected. The ATE class is expanded compared to EAL1, to include an analysis of the developer's own conducted testing on the interfaces of the product. The vulnerability analysis part is in scope, however this time aiming to validate the TOE's robustness against attacks of a higher potential (enhanced-basic). Finally, the ST and user guidance evaluation are performed at a very similar level compared with EAL1.

In the case of **EAL4 evaluations**, a few important updates are in place. Arguably the most important evaluation extension is the need for source code review, which means that the developer needs to make available the relevant source code of the TOE. Besides this, the most important other change compared with an EAL3 evaluation is the extended vulnerability analysis activity, which will aim to demonstrate that the TOE is resistant to attacks of a higher potential (moderate).





3.6. Evaluation meetings and deliverables

Under NSCIB, a Common Criteria evaluation includes up to three⁶ intermediate meetings, to share and discuss the results of the evaluation. The intermediate results are presented by the ITSEF, the presence of the sponsor in these meetings being optional.

Under the NSCIB process, certain deliverables are mapped to the intermediate evaluation meetings. **These deliverables are summarized in the table on the right.**

The table below provides a high level summary on the focus of the identified deliverables on the right.

Evaluation Meeting	Deliverables in Scope
Pre-EM1	<ul style="list-style-type: none"> IR_ASE Report
Guidance documentation creation	<ul style="list-style-type: none"> The ADV Presentation The ADV/AGD Reference Document The Configuration Item Identification Presentation
Development life-cycle	<ul style="list-style-type: none"> The ATE/AVA Test plan Presentation The ATE/AVA test descriptions The ALC Presentation
Secure Development procedures	<ul style="list-style-type: none"> The ATE/AVA test results The ALC Results Presentation Draft ETR
Post-EM3	<ul style="list-style-type: none"> Final ETR
Secure delivery procedures	Secure delivery procedures description
Testing	Developer test plan and test results
Source code review	Relevant source code of the TOE (if applicable based on selected EAL)

Deliverable	High Level Description
IR_ASE Report	Evaluation report focused on the analysis of the product's Security Target.
ADV Presentation	Presentation focused on analysing the architecture of the product, and its definition of subsystems and interfaces.
ADV/AGD Reference Document	Document detailing the most important evidence provided by the developer in terms of product architecture and user guidance.
Configuration Item Identification Presentation	Presentation analysing the parts of the TOE which are placed by the developer under configuration management.
ATE/AVA test plan presentation	Presentation aimed at summarizing the developer's own test results, plus proposing a test plan.
ATE/AVA test descriptions	Document highlighting the parameters of the developer's testing, as well as the proposed tests under the test plan.
ALC presentation	Presentation summarizing the conclusion after the analysis of the product's development processes, together with the proposed plan for validating these processes.
ATE/AVA test results presentation	Presentation focused on summarizing the results of the testing effort from the created test plan.
ALC Results presentation	Presentation detailing the results of the conducted validation of the developer's processes.
ETR	Evaluation Technical Report, summarizing the general overview and final results and conclusions of the evaluation.

⁶ Based on agreement with the scheme, the number of intermediate meetings can be decreased if the scope and type of the TOE allow for this

4. Harmonization of Common Criteria under the EU Cybersecurity Act

According to the recent European Cyber Security Act [8], the need for a harmonized European Certification scheme for ICT digital products, services and processes was established.

Upon request of the European Commission, based on Article 48 (2) of the Cybersecurity Act, ENISA⁷ has proposed the candidate EU Common Criteria scheme (EUCC) that is based upon the existing schemes operating under the SOG-IS Mutual Recognition Agreement [7]. The current intention is for the EUCC to become active in 2021. At that moment, all other national CC schemes shall stop producing certificates. A transition period shall be established to allow for the smooth migration from the current (national scheme based) CC evaluation approach, to the harmonized approach under the EUCC scheme.

In principle, the EUCC scheme will be strongly based on the CC evaluation standards and methodologies which are currently in use by national schemes. At the same time, the following highlights of the EUCC scheme are expressed:

- The EUCC will allow for possible reuse of results between certifications, facilitating a lean schedule and cost structure.
 - Under the EUCC two types of certificates will be issued, mapped to the Substantial and High assurance levels of the European Cybersecurity Act.
 - The selection of the assurance level (Substantial or High) will be based on the AVA_VAN level that will be used during the evaluation. The issued certificate will list the evaluated AVA_VAN level, together with the assurance level obtained.
 - The issued EUCC certificates will be directly recognized in all the EU member countries.
 - The validity of an EUCC certificate will be by default limited to five years.
- The general certification process will be very similar with the current one which makes use of national schemes. The main difference is that all the accredited Certification Bodies (CB) will be issuing the same type of resulting EUCC certificate, instead of the current scheme specific certificates. CBs will still rely on licensed and accredited ITSEFs for conducting the evaluation activities
 - The licensing requirements for the Certification Bodies and ITSEFs will stay similar to the current national CC schemes requirements
 - After the EUCC will be formally accepted, the formally agreed and on-going evaluations (under a specific national scheme) will be allowed to proceed, given that they can be finalized during the transition period
 - Certificates issued under certain certification schemes (including NSCIB) could be transformed into a certificate under the EUCC scheme if the necessary activities are conducted. ENISA may establish associated guidance to support the conditions for this transfer.



⁷ ENISA is the EU agency dedicated to achieving a high common level of cybersecurity across Europe

5. Further Clarifications

Common Criteria offers an extensive certification process and often requires additional clarifications on the certification procedures. Several questions are commonly encountered during discussion with interested developers. This section aims to summarize a set of topics which could provide additional clarity.

5.1. Process timeline

What is the average time frame required to perform the evaluation procedures and receive the final certificate for the product?

The timeline for the certification strongly depends on the desired evaluation level (EAL) for the product, as well as the scope and complexity of the product itself. Moreover, the timeline depends also on the agreements with the CC scheme, as their involvement will be necessary at least during the agreed evaluation meetings. While keeping these general disclaimers in mind, the following estimates (for an EAL1 – EAL4 evaluation) can be given concerning the duration of a project. These estimates consider the amount of time in between the start of the project (kick-off meeting) and the issue of the final certificate, in case of an evaluation which does not require additional evaluation rounds.

- **EAL1:** 2-3 months
- **EAL2:** 3-4 months
- **EAL3:** 4-6 months
- **EAL4:** 6-10 months

5.2. Costs

How much does it cost to certify the product based on CC?

The answer to this question depends very much on the type and complexity of the proposed TOE, as well as on the selected evaluation EAL level. Moreover, the costs are linked also to the quality of the available evaluation deliverables, as their low quality will trigger additional time for evaluation. With these aspects in mind, some estimates can be kept

in mind for an initial indication. In the case of an EAL3 evaluation, a range of 60.000 EUR to 90.000 EUR could be applicable. The deviation in this range is due to the possible differences in the scope and complexity of the product. Based on this reference, it is to be considered that lower evaluation levels (EAL1 and EAL2) will have less associated effort, therefore a lower total price. EAL4 evaluations come with additional required effort (especially linked with more testing and source code review) which will take the total price to a higher amount.

5.3. Choosing an EAL Level

What EAL level should be selected for a particular product?

This question is a very important one, as it impacts not only the timelines and effort of the evaluation, but of course also the final obtained certificate. In general, it is important, as a developer, to consider what is the aim for applying to a CC evaluation. If the aim is to obtain a general health check of the product based on a respectable evaluation methodology, then an EAL1 evaluation might be sufficient to satisfy this purpose.

If the aim is to match the certifications of the direct competitors, then the goal could be to look for at least the EAL level which these competitors have in place. Finally, if the goal is to finally sell the product to partners with strict security standards (such as for example governmental use or main telecommunication operators), then it would be advisable to look for an evaluation in the range of EAL3 or EAL4. Typically, for a software or embedded product, an EAL4 evaluation should be sufficient to demonstrate efficiently the robustness of the implemented security features. Higher levels of the CC (for example EAL5 and higher) are typically used by high risk products, including ICs, smart cards, military grade equipment, encryption devices, HSMs, etc. An evaluation laboratory (such as Secura) could help you with analysing the security posture of your product, recommending a particular EAL level for evaluation.

5.4. Creating the ST and necessary evaluation documentation

What is the best way to create a ST?

The best way to create a ST is to start with identifying the type of the product that needs to be certified. Based on the identified type of the product it is possible to identify if there exist a certified PP that can be considered as a basis for the draft of ST. Information about available certified PPs is available on CC portal via the link:

- <https://www.commoncriteriaportal.org/pps/>

Moreover, if the developer does not have an experience in working with Common Criteria, it is highly recommended to use a support of an evaluation laboratory to create the ST. A good quality ST is a critical element in the process of the evaluation, with direct implications on the duration of the evaluation.

Is the same approach mentioned for the ST applicable also to the rest of the required documentation?

Yes. The better the quality of the provided documentation, the smoother the general process will go. This will in turn translate to shorter timelines from the start of the project to the release of the certificate. The absence or lack of quality in the provided documentation will trigger delays in the process, as the intermediate meetings with the scheme might be postponed or repeated.

5.5. Additional consultancy services

Is it possible to arrange additional consultancy services by the evaluation laboratory? What is the process?

It is, however the evaluation laboratory needs to be extremely careful with the separation of the consultants and evaluators for a specific product. It is not allowed that the same persons who were involved in consultancy activities are further evaluating the resulting deliverables or the product. As long as this separation is made correctly and transparently, the NSCIB scheme allows for consultancy to take place.



5.6. Value of certification for the developer/sponsor

What are the benefits for the developer in certifying the product based on CC requirements?

There are several benefits for the developers to certify their products based on CC, which include:

- **Better market positioning**, since CC is an internationally recognised standard, known by many international stakeholders including government or private companies.
- **Acceptance of the CC certificates on the international level**, meaning there is no need to certify the product based on multiple CC schemes, which allows to save the costs on certification. For more details concerning the international mutual recognition of CC certificates, please refer to section 1.3.
- **Improved security posture of the product** and its development procedures with additional assurance in the security of the product based on the testing results performed by an independent party.
- **Validity of the issued certificate**, as the certificate will remain valid for a duration of 5 years, without the need to periodic renewal for the specific certified version of the TOE.
- **Possible advantage over direct competitors.** Depending on the type of TOE, direct competition with other companies could be an important aspect. If the target of this competition is access to institutions where security is a high asset (for example government or large scale private companies), then having a CC certificate on top of the competitors' offer could make an important differentiation.

5.7. Relation with the EU Cybersecurity act and new EUCC scheme

How will the obtained CC certificate relate to the new EUCC scheme?

Under the EUCC scheme, the already issued CC certificates will maintain their validity or will be converted to EUCC certificates, with minimal additional effort from the developer. Moreover, during the transition period after the introduction of the new EUCC scheme, all the CC evaluations which were previously started with a national CC scheme can be finalized with the issuing of a certificate. Therefore, from a developer point of view, there is little to no impact to the obtained certificate due to the transition to EUCC.



Interested in Common Criteria?

Secura pays close attention to the development around new security areas such as consumer IoT, energy, ICS SCADA or automotive. This results in services including well established certification schemes such as Common Criteria, IECEE or BSPA, but also new and relevant standards such as ETSI EN 303645 or IEC 62443.

Secura currently offers Common Criteria services under the Dutch NSCIB scheme. From this position, we are happy to help you with CC evaluation services, as well as consultancy on the product or the required documentation.

Please feel free to get in contact with our experts for a more detailed talk related to CC evaluations, as well as other possible relevant services for your products.






About Secura

Secura is your independent cybersecurity expert. Secura provides insights to protect valuable assets and data. We make cybersecurity tangible and measurable in the field of IT, OT and IoT. With security advice, testing, training and certification services, Secura approaches cybersecurity holistically and covers all aspects from people, policies, organizational processes to networks, systems, applications and data.

For more information, please visit: secura.com.

Keep updated with the latest insights on digital security and subscribe to our periodical newsletter: secura.com/subscribe.

Follow us on   

Contact us today at
info@secura.com or
visit secura.com for
more information.

SUBSCRIBE

TO OUR NEWSLETTER

Appendix A. List of References

1. Common Methodology for Information Technology Security Evaluation. Part 1: Introduction and general model. April 2017. Version 3.1, Revision 5.
2. Common Methodology for Information Technology Security Evaluation. Part 2: Security functional components. April 2017. Version 3.1, Revision 5.
3. Common Methodology for Information Technology Security Evaluation. Part 3: Security assurance components. April 2017. Version 3.1, Revision 5.
4. Common Methodology for Information Technology Security Evaluation. Evaluation methodology. April 2017. Version 3.1, Revision 5.
5. Netherlands Scheme for Certification in the Area of IT Security (NSCIB). NSCIB Scheme Procedure #1. Certification process. July 2019. Version 1.4.
6. Netherlands Scheme for Certification in the Area of IT Security (NSCIB). NSCIB Scheme Procedure #6. Evaluator Reporting during the Monitoring Phase. January 2020. Version 2.0.
7. SOG-IS. Mutual Recognition Agreement of Information Technology Security Certificates. January 2010. Version 3.0.
8. The EU 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.

Appendix B. Abbreviations

CC	Common Criteria
EM	Evaluation Meeting
ENISA	The European Union Agency for Cybersecurity
ETR	Evaluation Technical Report
EWP	Evaluation Work Plan
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

