EUROPEAN UNION AGENCY
FOR CYBERSECURITY


# EUCC SCHEME

## DRAFT STATE-OF-THE-ART DOCUMENT

### ACCREDITATION OF ITSEFs FOR THE EUCC SCHEME

Version 1.6b, June 2024

# DOCUMENT HISTORY

| Date | Version | Modification | Author's comments |
|---|---|---|---|
| June 2023 | 0.9 | Creation | Version submitted to the ECCG |
| August 2023 | 1.0 | Addition of a document history section with a link to the SOG-IS document the state-of-the-art document is based on, where applicable<br>Rephrasing of subcontracting and non compliance conditions<br>Addition of cryptography in Annex | Based on comments received |
| October 2023 | 1.1 | | Approved for publication on 20/10/2023 by the ECCG and the European Commission |
| April 2024 | 1.2 | Clarification of requirements related to independence and consultancy | Version submitted to ECCG comments |
| 29 April 2024 | 1.3 | New clarification of requirements related to independence and consultancy<br>Addition of a transition chapter | Update based on latest ECCG comments received after the ECCG meeting of April 15<br>Version submitted to EA |
| 30 April 2024 | 1.4 | Deletion of the EA table<br>Additional clarification of requirements related to independence and consultancy, including EUCC related examples | Update based on EA inputs<br>Version submitted to ECCG comments |
| 23 May 2024 | 1.5 | Alignement of the Legal Information and the Introduction chapter with the SoA document related to the Accreditation of CBs for the EUCC scheme<br>Additional clarification of requirements related to independence and consultancy<br>Clarification of the scope of the accreditation<br>Addition of annex B on 'Collection of developer evidence' according to the equivalent SOG-IS document | Update based on EA, ECCG and CABs inputs<br>Version submitted to ECCG and EA comments |
| 4 June 2024 | 1.6a | Clarification of the scope of the accreditation (chapter 5)<br>Clarification of the independence requirement (chapter 6.2.1)<br>Minor correction of Annex A2.2 title<br>Correction of typos | Update based on EA and ECCG comments<br>Version submitted to ECCG endorsement |
| 21 June | 1.6b | Minor correction in the table in chapter 6.1<br>Deletion of the standards reference dates<br>Re-clarification of the independence requirement (chapter 6.2.1)<br>Transposition of the references to the EUCC candidate scheme to references to the EUCC implementing regulation | Endorsed and approved for publication on 16/07/2024 by the ECCG |

# LEGAL INFORMATION

## LEGAL NOTICE

This publication is established in accordance with recital 18 of Commission Implementing Regulation (EU) 2024/482**.**

***This draft version of the state-of-the-art document is published for information only. After endorsement by the ECCG, it has been submitted for inclusion in the list of applicable state-of-the-art documents listed in Annex I of Commission Implementing Regulation (EU) 2024/482. It has received a positive opinion from the ECCG but has not yet been adopted by the Commission via an amendment of the Implementing Regulation (EU) 2024/482. State-of-the-art documents will only become applicable and legally binding following their inclusion in the Implementing Regulation and in line with relevant transition rules specified by such Regulation. Therefore, this document should not yet be considered as final and legally binding. Furthermore, changes might be introduced in state-of-the-art documents in the context of the comitology procedure.***

The document shall be updated where developments and best practices in the field of accreditation require to do so. Updates of this document shall be submitted to the ECCG.

This document shall be read in conjunction with Regulation (EU) 2019/881, the Commission Implementing Regulation (EU) 2024/482, its annexes and where applicable supporting documentation that is made available.

This document is made publicly accessible through the EU cybersecurity certification website and is free of charge.

ENISA is not responsible or liable for the use of the content of this document. Neither ENISA nor any person acting on its behalf or on behalf for the maintenance of the scheme is responsible for the use that might be made of the information contained in this publication.

## COPYRIGHT NOTICE



## CONTACT

Constructive feedback or questions related to this document are welcome, please use Cybersecurity Certification (europa.eu)

# CONTENTS

# 1 INTRODUCTION

This draft state-of-the-art document as defined under Article 2 point 14 of Regulation (EU) 2024/482 is a legal supporting document under Implementing Regulation (EU) 2024/482 on establishing the Common Criteria-based cybersecurity certification scheme (EUCC). It provides requirements related to the accreditation of ITSEFs, as defined in the scheme, that shall establish they are technically competent for their related tasks according to the Common Criteria in conjunction with the Common Evaluation Methodology.

This technical competence shall be assessed through the accreditation of the ITSEFs by a National Accreditation Body (NAB) as per ISO/IEC 17025, the standard selected for the accreditation of ITSEFs by the EUCC scheme.

As ISO/IEC 17025 applies to a very general and wide range of testing activities, this document provides necessary interpretations of the standard and of EUCC specific requirements for ITSEFs whose conformity is to be assessed during their accreditation.

This document shall be used by National Accreditation Bodies to support their compliance assessments.

## 1.1 RESPONSIBILITIES OF THE NATIONAL ACCREDITATION BODY

The NAB that is established in a Member State in accordance with Regulation (EC) 765/2008, is the body that is responsible to perform the accreditation for a conformity assessment body (the Certification Body (CB) and the Information Technology Security Evaluation Facility (ITSEF) both need to be accredited for their conformity assessment activities) (Article 60 (1) CSA).

Where the ITSEF intends to evaluate for the assurance level high, the NCCA and the NAB should pay attention to the fact that the ITSEF may want to avoid duplication of effort and to use the work undertaken during the accreditation process as much as possible in the authorization process. Therefore, the accreditation body should, wherever practical, use technical assessors (TAs) and technical experts (TEs) who can also be accepted by the NCCA and should consult with the NCCA if they are interested in including a suitable technical expert to participate in the accreditation process. TAs and TEs used by the NAB shall however operate under the sole responsibility of the NAB for their accreditation activities.

In addition, the following tasks need to be performed by the NAB:

- Reporting the results of the accreditation assessment to the NCCA, including assessment reports and decisions of granting, extending, reducing, suspending, or withdrawing of accreditations for EUCC;
- Apply an assessment program to assess that the accredited conformity assessment bodies meet the requirements of accreditation;
- Take appropriate measures to reduce the scope of accreditation, suspend or withdraw the accreditation of conformity assessment bodies where they are non-compliant with the accreditation requirements including those coming from the CSA.

  In the situation of possible infringements of the CSA, particularly related to the requirements of Annex of the CSA, the collaboration with the NCCA is important as the NCCA has the monitoring and supervising powers under Article 58 (8) CSA that can support the NAB in this task.

## 1.2 RESPONSIBILITIES OF THE NATIONAL CYBERSECURITY CERTIFICATION AUTHORITY

Based on the accreditation decision established by the NAB, the NCCA shall establish a notification (Article 61 CSA) to the European Commission according to an ECCG approved template and inform ENISA, and notify as well any subsequent change in the status of the accreditation: reduction of the scope, suspension or withdrawal of the accreditation, so that ENISA can maintain the accreditation information publicly available on the European cybersecurity certification website.

The monitoring and supervising national cybersecurity certification authorities (NCCAs) have the responsibility to actively assist and support the NAB in their monitoring and supervising tasks and need to share information and report to the NAB. This shall occur without prejudice to the handling of complaints performed by the ITSEF in accordance with ISO/IEC 17025 with regards to:

- Any (potential) non-compliance of the ITSEF related to the accreditation requirements annexes to regulation (EU) n°2029/881 (Cybersecurity Act- Article 58 (7) (c) and Article 58 (7) (h, i) CSA);
- Any complaints received related to the authorization of a ITSEF that may have an impact on the accreditation of the ITSEF (for assurance level ‘high’ Article 58 (7) (f) CSA).

The NCCA needs to include the active assistance and support provided to the NAB with regards to the monitoring and supervision of the activities of CABs (CBs & ITSEFs), in accordance with Article 17 (4) Commission Implementing Regulation (EU) 2024/482 in an annual summary report and send this to the European cybersecurity certification group (ECCG) and the EU Agency for Cybersecurity (ENISA)[1].

## 2 NORMATIVE REFERENCES

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)

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council

Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93

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)

Implementing Regulation (EU) 2024/482 on establishing the Common Criteria-based cybersecurity certification scheme (EUCC)

ISO/IEC 15408 - Information technology - Security techniques - Evaluation criteria for IT security, further referenced as Common Criteria for Information Technology Security, or CC

ISO/IEC 18045 - Information technology - Security techniques - Methodology for IT security evaluation, further referenced as Common Evaluation Methodology, or CEM

ISO/IEC 17025 - General requirements for the competence of testing and calibration laboratories

ISO/IEC 17065 - Conformity assessment - Requirements for bodies certifying products, processes and services

ISO/IEC 19896-1 - IT security techniques - Competence requirements for information security testers and evaluators - Part 1: Introduction, concepts and general requirements

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 TS 23532-1 - Information security, cybersecurity and privacy protection — Requirements for the competence of IT security testing and evaluation laboratories — Part 1 Testing and evaluation for ISO/IEC 15408

## 3 ACRONYMS AND DEFINITIONS

### 3.1 ACROMNYMS

CAB Conformity Assessment Body
CB Certification Body
CC Common Criteria for Information Technology Security Evaluation.

[1] See Article 58 (7) (g) CSA.

| | |
|---|---|
| CEM | Common Methodology for Information Technology Security Evaluation |
| CSA | Cybersecurity Act |
| EAL | Evaluation Assurance Level |
| EC | European Commission |
| ENISA | European Union Agency for Cybersecurity |
| ETR | Evaluation Technical Report |
| EU | European Union |
| GDPR | General Data Protection Regulation |
| ICT | Information and communications technology |
| IEC | International Electrotechnical Commission |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| ITSEF | Information Technology Security Evaluation Facility |
| NAB | National Accreditation Body as defined in point (11) of Article 2 of Regulation (EC) No 765/2008; |
| NCCA | National Cybersecurity Certification Authority |
| PP | Protection Profile |
| SFR | Security Functional Requirement |
| SMEs | Small and Medium Enterprises |
| SOG-IS | Senior Officials Group Information Systems Security |
| ST | Security Target |
| TOE | Target of evaluation |
| TS | Technical Specification |
| TSFI | TOE security function interfaces |

## 3.2 DEFINITIONS

The definitions used under Article 2 of Regulation (EU) 2019/881 (hereinafter referred to as CSA) and under Article 2 of the Implementing Regulation (EU) 2024/482 apply to this document, in particular the following definitions

**Conformity Assessment Body**
"Conformity assessment body (CAB)" means a conformity assessment body as defined in point (13) of Article 2 of Regulation (EC) No 765/2008: 'conformity assessment body' shall mean a body that performs conformity assessment activities including calibration, testing, certification and inspection;

**Certification Body**
"Certification Body (CB)" means and entity of a CAB described under Article 2 (13) of Regulation (EC) No 765/2008 performing certification activities or activities of the national cybersecurity certification authority (NCCA) related to the issuance of European cybersecurity certificates referred to in Article 56(5)(a) CSA (see Article 2 (4) EUCC) ).

Under provisions of Art. 58(4), a NCCA responsible for, or issuing certifications is considered to be a CB when it is involved in certification under assurance level 'high'. The CB can therefore be a private entity or public body under EUCC.

**Evaluation**
"Evaluation" means an assessment of the applicant's claimed Security Funtional Requirements associated with the assessed ICT product or a Protection Profile by the use of Security Assurance Requirements as referred to in the EUCC, in order to determine whether the claims made are justified. This implies under ISO/IEC the combination of the selection and determination functions of conformity assessment activities (ISO/IEC 17065).

Evaluation tasks can include activities such as design and documentation review, sampling, testing, inspection and audit (ISO/IEC 17065).

In the context of the EUCC, 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).

Evaluation activities are performed by an ITSEF, while the Certification Body is focusing on the performance of review, decision making related to issuance, extension and reduction of the scope of certifications, suspension and withdrawal of a certificate, attestation, complaint handling and monitoring of certain compliance obligations of holders of a certificate.

**ITSEF**
"ITSEF" means an Information Technology Security Evaluation Facility, which is an entity of a CAB described under Article 2(13) Regulation (EC) 765/2008 performing calibration, testing or sampling activities associated with subsequent calibration or testing and related to necessary inspection activities. Third-party CAB that performs one or more of the following activities: - calibration - testing - sampling, associated with subsequent calibration or testing (ISO/IEC 17025).

In the context of the EUCC, an ITSEF carries out selection and determination functions as a part of conformity assessment evaluation activities.

The ITSEF can be a body that together with the CB forms one legal entity. It can also be a separate legal entity that is subcontracted by a CB to perform the activities described in the definition.

Where requirements are defined in the EUCC for an ITSEF, they shall apply to both the body that together with the CB forms one legal entity and as well to the ITSEF that is a subcontracted legal entity.

In the context of the EUCC, the ITSEF is required to meet the requirements of standard ISO/IEC 17025 and the CB needs to meet the requirements of standard ISO/IEC 17065.

**Evaluator**
ITSEF personnel performing evaluation activities.

## 4 APPLICABILITY OF INTERNATIONAL STANDARDS TO THE ACCREDITATION OF ITSEFS

The CSA prescribes the obligation that schemes refer to international, European, or national standards that are to be 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.

In this respect, it shall be taken into account that the following standards apply to the accreditation of ITSEFs:

- ISO/IEC 17025 - General requirements for the competence of testing and calibration laboratories: meeting this standard is mandatory for ITSEF accreditation.
- ISO/IEC TS 23532-1 - Information security, cybersecurity and privacy protection - Requirements for the competence of IT security testing and evaluation laboratories - Part 1 Testing and evaluation for ISO/IEC 15408: this standard that provides an interpretation of ISO/IEC 17025 shall also apply for ITSEF accreditation.

Note: ISO/IEC TS 23532-1 references to "scheme owner(s)" should be understood in this context as referring to the related accredited and, if applicable authorized CB and NCCA.

- Additions to some ISO/IEC TS 23532-1 requirements are defined in this document, that are also mandatory for ITSEF accreditation.
- Additional competence requirements are defined in this document, based on ISO/IEC 19896- IT security techniques - Competence requirements for information security testers and evaluators, both parts 1 and 3, that provide the definition of elements of competence, competency levels and the measurement of the elements of competence, that are to be applied by ITSEFs.

Note: ISO/IEC 19896 provides some informative annexes that provide guidance on the competence requirements for information security evaluators. Some of these annexes are identified as mandatory in this document as detailed in the chapter "Accreditation requirements".

EUCC scheme requirements that apply to ITSEFs are also included in this document, so that their compliance can be assessed during the accreditation process.

# 5 SCOPE OF ITSEF ACCREDITATION

The scope of the ISO/IEC 17025 accreditation for EUCC ITSEFs shall be based on the following standards:

- the CC
- the CEM

These standards define security functional and assurance components and corresponding evaluation activities. Such components and activities are packaged in the so-called Evaluation Assurance Levels.

The scope of the accreditation shall include the evaluation activities from the CC in which the ITSEF has proven technical competence, named and grouped by the rules of the referred standards.

Only the information described as “Type of test and test parameter” shall vary depending on the scope of accreditation that is requested and granted.

The requirements for accreditation do not deal directly with different types of technology being tested but focus on an assessment of the specific competences that the ITSEF needs to define and demonstrate in accordance with the applicable standards and the requirements defined under Annex I CSA.

The scope of accreditation shall therefore at least specify:

- The testing field:
  - ICT Cybersecurity Evaluation
- The test object, product or process, for example:
  - Information and Communication Technology Products, within the following categories:
    - Smartcards and similar devices
    - Hardware devices with security boxes
    - Generic software and network products
- The type of test and test parameter, for example:
  - IT security evaluation up to EAL3 augmented with ALC_FLR.2
- The reference to the scheme:
  - EUCC

Technology and evaluation technique types from Annex A in which the ITSEF has proven technical competence shall be detailed in the accreditation assessment report.

# 6 ACCREDITATION REQUIREMENTS

The EUCC scheme ITSEF accreditation requirements that shall apply are the following:

- The requirements for the competence of testing and calibration laboratories defined in ISO/IEC 17025 complemented by the requirements defined in ISO/IEC TS 23532-1.
- Those requirements that are to be met by conformity assessment bodies indicated in the Annex of the CSA, to the extent applicable to the ITSEF activities. These are provided in section “General accreditation requirements from the [CSA]”.
- The requirements specified in this document, as provided in section “Specific accreditation requirements”, based on those requirements applicable to ITSEFs indicated in the EUCC - except those related to authorization.

## 6.1 GENERAL ACCREDITATION REQUIREMENTS FROM THE CSA

Conformity assessment bodies that wish to be accredited shall meet the requirements indicated in the Annex of the CSA, included in the following table. Considering the role of the ITSEF to evaluate and not to certify the ICT products, this table specifies to which extent the requirements apply to the ITSEF, and provides links to related requirements

from ISO/IEC 17025 that may support compliance to the indicated CSA requirements in the second column of the table.

| Requirement from CSA Annex "REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES" | | Supporting ISO/IEC 17025 requirement |
|---|---|---|
| 1. | A conformity assessment body shall be established under national law and shall have legal personality. | ISO/IEC 17025, 5.1 |
| 2. | A conformity assessment body shall be a third-party body that is independent of the organisation or the ICT products, ICT services or ICT processes that it assesses. | ISO/IEC 17025, 4.1<br>Independance |
| - | | |
| 3. | A body that belongs to a business association or professional federation representing undertakings involved in the design, manufacturing, provision, assembly, use or maintenance of ICT products, ICT services or ICT processes which it assesses may be considered to be a conformity assessment body, provided that its independence and the absence of any conflict of interest are demonstrated. | ISO/IEC 17025, 4.1 |
| 4. | The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the ICT product, ICT service or ICT process which is assessed, or the authorised representative of any of those parties. That prohibition shall not preclude the use of the ICT products assessed that are necessary for the operations of the conformity assessment body or the use of such ICT products for personal purposes. | ISO/IEC 17025, 4.1<br>Impartiality |
| 5. | The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, manufacture or construction, the marketing, installation, use or maintenance of the ICT products, ICT services or ICT processes which are assessed, or represent parties engaged in those activities. The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to their conformity assessment activities. That prohibition shall apply, in particular, to consultancy services. | ISO/IEC 17025, 4.1<br>Impartiality |
| 6. | If a conformity assessment body is owned or operated by a public entity or institution, the independence and absence of any conflict of interest shall be ensured between the national cybersecurity certification authority and the conformity assessment body, and shall be documented. | |
| 7. | Conformity assessment bodies shall ensure that the activities of their subsidiaries and subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities. | ISO/IEC 17025, 4.1<br>ISO/IEC 17025, 4.2<br>ISO/IEC 17025, 6.6.2 |

| Requirement from CSA Annex "REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES" | | Supporting ISO/IEC 17025 requirement |
|---|---|---|
| | | Impartiality<br><br>Confidentiality |
| 8. | Conformity assessment bodies and their staff shall carry out conformity assessment activities with the highest degree of professional integrity and the requested technical competence in the specific field, and shall be free from all pressures and inducements which might influence their judgement or the results of their conformity assessment activities, including pressures and inducements of a financial nature, especially as regards persons or groups of persons with an interest in the results of those activities. | ISO/IEC 17025, 4.1<br><br>Impartiality<br><br>ISO/IEC 17025, 6.2.3<br><br>Competence |
| 9. | A conformity assessment body shall be capable of carrying out all the conformity assessment tasks assigned to it under this Regulation, regardless of whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility. Any subcontracting to, or consultation of, external staff shall be properly documented, shall not involve any intermediaries and shall be subject to a written agreement covering, among other things, confidentiality and conflicts of interest. The conformity assessment body in question shall take full responsibility for the tasks performed. | ISO/IEC 17025, 6.6 |
| 10. | At all times and for each conformity assessment procedure and each type, category or sub-category of ICT products, ICT services or ICT processes, a conformity assessment body shall have at its disposal the necessary: | ISO/IEC 17025, 6.2<br><br>ISO/IEC 17025, 7.2 |
| (a) | staff with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks; | |
| (b) | descriptions of procedures in accordance with which conformity assessment is to be carried out, to ensure the transparency of those procedures and the possibility of reproducing them. It shall have in place appropriate policies and procedures that distinguish between tasks that it carries out as a body notified pursuant to Article 61 and its other activities; | |
| (c) | procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the technology of the ICT product, ICT service or ICT process in question and the mass or serial nature of the production process. | |
| 11. | A conformity assessment body shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner, and shall have access to all necessary equipment and facilities. | ISO/IEC 17025, 6.3<br><br>ISO/IEC 17025, 6.4 |
| 12. | The persons responsible for carrying out conformity assessment activities shall have the following: | ISO/IEC 17025, 6.2<br><br>Competence |

| Requirement from CSA Annex "REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES" | | Supporting ISO/IEC 17025 requirement |
|---|---|---|
| (a) | sound technical and vocational training covering all conformity assessment activities; | |
| (b) | satisfactory knowledge of the requirements of the conformity assessments they carry out and adequate authority to carry out those assessments; | |
| (c) | appropriate knowledge and understanding of the applicable requirements and testing standards; | |
| (d) | the ability to draw up certificates, records and reports demonstrating that conformity assessments have been carried out. | |
| 13. | The impartiality of the conformity assessment bodies, of their top-level management, of the persons responsible for carrying out conformity assessment activities, and of any subcontractors shall be guaranteed. | ISO/IEC 17025, 4.1<br>Impartiality |
| 14. | The remuneration of the top-level management and of the persons responsible for carrying out conformity assessment activities shall not depend on the number of conformity assessments carried out or on the results of those assessments. | ISO/IEC 17025, 4.1 |
| 15. | Conformity assessment bodies shall take out liability insurance unless liability is assumed by the Member State in accordance with its national law, or the Member State itself is directly responsible for the conformity assessment. | |
| 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. | ISO/IEC 17025 4.2<br>ISO/IEC TS 23532-1<br>Confidentiality |
| 17. | With the exception of point 16, the requirements of this Annex shall not preclude exchanges of technical information and regulatory guidance between a conformity assessment body and a person who applies for certification or who is considering whether to apply for certification. | |
| 18. | Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, taking into account the interests of SMEs in relation to fees. | |
| 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 | This point does not apply to ITSEFs, see point 20. |

| Requirement from CSA Annex "REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES" | Supporting ISO/IEC 17025 requirement |
|---|---|
| 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. | ISO/IEC 17025 |

## 6.2 SPECIFIC ACCREDITATION REQUIREMENTS

In addition to the requirements included in ISO/IEC 17025 and ISO/IEC TS 23532-1, the following requirements apply to the accreditation of an EUCC ITSEF.

### 6.2.1 Independence

The independence criteria from CSA Annex point 2 shall be applied to the ITSEF but not to the entire legal entity (if the ITSEF is part of a bigger legal entity) and apply to the ICT product, ICT process, ICT service under evaluation.

The ITSEF shall not:

- be the designer, manufacturer, installer, distributer or maintainer of the assessed ICT product;
- be the designer, implementer, operator or maintainer of the assessed ICT process;
- be the designer, implementer, provider or maintainer of the assessed ICT service;
- offer or provide consultancy activities, which are in conflict with their independence of judgement or integrity in relation to their conformity assessment activities according to ISO/IEC 17025 to its clients.

This does not preclude:

- the possibility of exchange of information (e.g.: explanations of findings or clarifying requirements) between the ITSEF and its clients;
- the use, installation and maintenanceof assessed ICT products which are necessary for the operations of the ITSEF.

The ITSEF shall inform its clients of any activity of its legal entity including being a designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the ICT product, ICT service or ICT process that might be related to the type of products of the clients.

### 6.2.2 Impartiality

ISO/IEC 17025, "4.1 Impartiality"

The ITSEF must ensure a strict separation of its responsibilities to maintain impartiality. This can be achieved within the same legal entity by meeting the requirements of EN ISO/IEC 17025 for impartiality. Additionally, an ITSEF is required to implement an ongoing risk analysis process to continuously assess its risks.

The following list of activities (which builds on EA-2/20 G: 2020[2]) of the ITSEF shall not be considered as "consultancy":

a) Preparation of evaluation documentation and evidence in accordance with the rules defined in Annex B 'Collection of developer evidence'.
b) Providing general training or guidance on best practices and state-of-the-art, under the following condition:
   - This activity shall exclude recommendations regarding the implementation of a specific architecture or mechanism.

[2] https://european-accreditation.org/?s=ea-2%2F20

c) Providing technical analysis of product failures (including vulnerabilities), under the following conditions:
   - The scope shall be clearly presented in the contract;
   - The delivery of the activity shall be limited to diagnosis;
   - The ITSEF personnel shall commit to not recommend solutions and this commitment shall be recorded by the ITSEF.

d) Participation to R&D projects, studies and to the maintenance of the EUCC scheme related to or emcompassing the categories of ICT products and technologies for which the ITSEF is accredited (e.g.: high level study into general market/design/production trends within the overall sector, feasibility studies on certification schemes reusing EUCC certification, mapping between EUCC certification and other regulations, participation to the definition and update of EUCC state-of-the-art documents and guidance), under the condition that:
   - The ITSEF shall allow the results to be made publicly available.

e) Development of tools for certification activities (e.g.: tools to support the development of PPs or STs, test benches, code review tools), including the possibility to register a patent and/or a user licence for it, under the conditions that:
   - The ITSEF shall establish an analysis before project launch in order to verify there is no impact on conformity assessment or on assessed parties which might be competitors;
   - The activity shall relate to the complete sector, and shall neither be for the ITSEF nor for an individual industrial, and the ITSEF shall provide collective and transparent communication;
   - There shall not be subsequent certification of a ICT product related to a patent;
   - There shall not be any user licence resulting in collective certification.

f) Delivery of services that could be conformity assessment but out of the accreditation scope with regard to notification (e.g. Common Criteria assessment of a product outside EUCC certification process for national security purpose).

g) Development of a test protocol (e.g.: development of a test bed to develop ITSEFs' and/or CBs' skills or to support and/or monitor their accreditation or authorisation), under the conditions that:
   - The validation of the method shall satisfy the requirements of ISO/IEC 17025;
   - The ITSEF shall provide a generic test or inspection protocol, and make it publicly available, or;
   - The ITSEF may only provide a specific test or inspection protocol that is non publicly available for the benefit of evaluation and certification activities outside of its scope of accreditation.

Where an activity is considered as acceptable with conditions, the ITSEF shall demonstrate the fulfillment of conditions and provide detailed proofs of this to the NAB.

### 6.2.3 Confidentiality

EUCC, Recital 27 & Article 43 Protection of information
ISO/IEC 17025, "4.2 Confidentiality"

#### Additional requirement to ISO/IEC TS 23532-1, 4.2.6

The exclusions indicated by ISO/IEC TS 23532-1, 4.2.6 need to be noted and justified in the ETR to the responsible CB. If the responsible CB considers that access to this information is relevant to perform the certification decision, it can be a cause for rejecting the requested certificate.

The ETR for composition needs to include all information necessary for the composition. It has to be technically relevant, while taking into account the confidentiality of sensitive information.

#### Additional requirement to ISO/IEC TS 23532-1, 4.2.8

The scope of the policies, procedures and security manual to ensure the protection of proprietary information shall also cover and protect the following:

a) Handling of personal data, where applicable.
b) Information necessary for
   – the effective implementation of the EUCC scheme, in particular for the purpose of accreditation assessments,

- effective collaboration between the involved authorities and bodies,
- the handling of publicly unknown and subsequently detected vulnerabilities in the TOE in the process of, or after certification, and,
- the handling of complaints.

c) The case of subcontracting, and in the situation where the 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 as well as the relevant know-how and evaluation and testing approaches and their results of the ITSEF.

d) Protection under scenarios of unavailability or lack of accessibility of the ITSEF main location; in particular, remote evaluation activities, both from the home-office of the evaluators, or from the manufacturer site, shall be adequately protected.

e) The ITSEF should ensure that information that is required by a user or users (i.e. those accessing the evaluation information) for a short period, is retrievable when this period expires.

f) The ITSEF shall implement mechanisms that allow setting a fixed duration for users' access to confidential information.

Confidential information that requires temporary access to be given to a set of users to perform a specific task such as assessments from NABs should not be permanently handed to the possession such temporary users. They should only have access for the duration of the activity.

g) Confidential information about an evaluation activity should be restricted to the ITSEF staff involved in the specific evaluation activity.

In particular, the policies, procedures and security manual to ensure the protection of proprietary information shall also cover and include the following measures:

a) The information system shall include tools that provide encryption functionalities for non-public Information at rest. These tools should be referenced by an ENISA or a National guidance document.
Encryption tools that are deployed for security of information are expected to be in compliance with, by order of precedence:
   - EU and national regulation regarding the protection of sensitive information,
   - recommendations, guidance and opinions from the competent cybersecurity authorities of the Member State,
   - recommendations from the ECCG.

b) Secure electronic storage and communication must be achieved for non-public Information through accepted and recognised cryptographic methods and algorithms. The ITSEF shall refer to and comply with ENISA or National cryptography guidelines for further guidance.

c) ITSEF staff shall be trained on information handling and sign agreements of compliance with information security obligations to maintain data secrecy. The ITSEF shall keep these agreements as per Retention of records requirements.
Every staff member shall sign an NDA before he/she is granted access to non-public information. In governmental organizations where there are binding legal regulations on information secrecy, these rules shall be leading, unless they interfere with EU law.
The ITSEF shall maintain a updated information security workshop schedule for staff involved in the EUCC scheme process. The workshop shall be performed on a regular basis and include updates on relevant regulatory changes.

Evaluation contracts between ITSEFs and their customers shall identify which parties will have access to the evaluation evidence and findings that are part of the certification process and that have for the purpose of certification and certification maintenance of the ICT product and compliance, a need-to-know right, subject to accreditation assessments and/or other scheme defined processes and procedures. The CB, the NAB where necessary for the purpose of accreditation, and the NCCA where necessary for the purpose of its monitoring and supervision tasks, shall be informed about these contract obligations.

### 6.2.4 Competence

EUCC, Recital 19 & Article 23 Notification of certification bodies
ISO/IEC 17025, "6.2 Personnel"

The ITSEF, their evaluators and, if applicable, the relevant staff of their subcontracted parties shall be required to have the necessary expertise and experience in performing the specific testing activities to determine the product's resistance against specific attacks (penetration testing).

The ITSEF shall define and operate a competence management system for the evaluators where:

- The elements of competence, competency levels and the measurement of the elements of competence are drawn from ISO/IEC 19896-1, and if they differ, they shall be commensurate with the objectives that are defined and at least be equivalent to the elements defined by ISO/IEC 19896-1. The ITSEF needs to demonstrate this.
- The knowledge, skills, experience and education, and the applicable requirements for the evaluators are drawn from ISO/IEC 19896-3, and if they differ, they shall be commensurate with the objectives and be at least equivalent to the requirements defined by ISO/IEC 19896-3. The ITSEF needs to demonstrate this.
- The knowledge required for evaluating security assurance requirement classes is specified based on Annex B of ISO/IEC 19896-3.
- The knowledge required for evaluating security functional requirement classes is specified based on Annex C of ISO/IEC 19896-3.
- The knowledge required for evaluating specific technologies and exercising different evaluation technique types are to be specified by the ITSEF using the classification provided in Annex.
  The ITSEF may use other classification criteria, as long as it can be mapped to the one provided in Annex. Such mapping, and the supporting rationale, shall be made available to the CB the ITSEF is subcontracted with, the NABs and NCCA.

### 6.2.5 Facilities

EUCC, Recital 27 & Article 43 Protection of information
ISO/IEC 17025, "6.3 Facilities and environmental conditions"

Additional requirement to ISO/IEC TS 23532-1, 6.3.1.1

Network isolation must ensure the integrity of the test results and their confidentiality.

### 6.2.6 Subcontracting

ISO/IEC 17025, "6.6 Externally provided products and services"

The ITSEF shall operate according to defined procedures ensuring that:

- The use of a subcontracted third-party facility is outlined in the evaluation plan, approved by the manufacturer or provider and by the CB and compliant with the obligations under the CSA, Annex 1 of the CSA and the EUCC while the ITSEF remains responsible for the work done. The subcontacted third-party shall be subject to the accreditation procedure for the subcontracted tasks it is performing;
- If the ITSEF uses equipment at a third-party facility as specified in the sub-contracting, the evaluator shall be present and instruct the equipment operating personnel. To instruct the operating personnel, evaluators shall have the required knowledge of the subcontract with the third-party, the TOE, the equipment, and the purpose and scope of the evaluation.

### 6.2.7 Non-compliance

EUCC, Article 31 Consequences of non-compliance by the conformity assessment body
The ITSEF shall support the CB's, for which it performed evaluation activities, in their handling of non-compliances in the conditions under which the evaluation of the certification takes place, by defining and operating a process where:

- They identify within the scope of their tasks potentially impacted certified ICT products, from those TOEs evaluated by the ITSEF that contributed to the certification of the ICT product.
- They perform where deemed necessary by the CB, or at the discretion of the NCCA, a series of re-evaluation tasks on one or more certified ICT products.

- If the ITSEF that performed evaluation activities on behalf of a certified product, proves to be non-compliant, the NCCA handling the non-compliance with the responsible CB may appoint an other supporting ITSEF to perform certain evaluation activities.

### 6.2.8 Retention of records

EUCC, Article 40 Retention of records by certification bodies and the ITSEF
ISO/IEC 17025, “7.5 Technical records”, “8.4 Control of records”

The record system shall include all records and other related documents produced in connection with each evaluation; the recording shall be updated, accurate and complete to enable the course of each evaluation to be traced and reproduceable.

All records shall be securely and accessibly stored for a period of at least five (5) years after the final date of the certificate validity, with the exception of running investigations related non-compliance and complaint handling and their respective legal remedy procedures.

All records related to the handling of non-compliances and/or complaints not related to the evaluation shall be kept for a period of at least five (5) years after the non-compliance and/or complaint was handled and all related (legal) procedures are closed.

In case a different expiration date of the certificate has been attributed in accordance with the conditions of EUCC, SECTION II ISSUING, RENEWING AND WITHDRAWING EUCC CERTIFICATES FOR PROTECTION PROFILES, it shall be taken into account for the new calculation of the retention period of the records, with the same rules in this section.

New or revised information related to the activities described under that Section of the EUCC shall be added to the previous records for the evaluation.

### 6.2.9 Ensuring the validity of results

ISO/IEC 17025, “7.7.2 Monitoring of laboratory performance”

This clause requires that a laboratory shall monitor its performance by comparison with the results of other laboratories. In particular, the ITSEF needs to demonstrate that it is having a planning and where already the benchmarking is performed a demonstrated proof of participation and result report.

Further guidance is needed how to apply this requirement on CC laboratories, also to ensure a level playing field within Europe.

### 6.2.10 Management System documentation

ISO/IEC 17025, “8.2 Management system documentation (Option A)”

Additional requirement to ISO/IEC TS 23532-1, 8.2.8

Procedures for evaluation should be written with a level of detail that would allow a technical competent evaluator to perform the evaluation without further guidance.

### 6.2.11 Quality process

EUCC, “11. RULES FOR MONITORING COMPLIANCE”
ISO/IEC 17025, “8.8 Internal audits”

The management process of the ITSEF shall explicitly ensure conformity with all the applicable requirements and obligations of the EUCC, including the requirements associated to handle complaints.

### 6.2.12 Composite evaluations

EUCC, Article 7 Evaluation criteria and methods for ICT products

The ITSEF shall operate according to defined procedures that ensure that, where an ICT product undergoes a composite product evaluation, necessary including where needed sensitive information that is reused from the initial

evaluation is provided to the ITSEF performing the composite evaluation. This information shall be shared in the form of an evaluation technical report (ETR) for composition, based on the template provided by ENISA.

The information sharing in the case of composite evaluation must take place in full cooperation between the CBs, i.e. the CB that has certified the base component and the one handling the composite evaluation.

Besides the relevant documentation which should be exchanged, there must exist a communication channel between all involved parties to clarify technical problems. All parties/bodies, esp. the ITSEF which is responsible for the composition ETR must support this approach.

### 6.2.13 Monitoring compliance

EUCC, Article 27 Monitoring activities by the holder of the certificate

Manufacturers, developers and any other holders of a cybersecurity certificate shall have procedures and processes in place that allow to demonstrate their continued compliance with the specified cybersecurity requirements under their certification.

The CB must carry out an assessment of the criticality of the reported irregularities with the support of the ITSEF if necessary.

To support compliance monitoring, ITSEFs shall define a set of compliance monitoring processes that ensure that, for TOEs evaluated by the ITSEF:

- They carry out an active cybersecurity-oriented technology watch, and keep themselves informed and continuously updated on the main discovered vulnerabilities and attack techniques relevant to their scope of assessment,
- They systematically carry out a search for publicly known vulnerabilities in connection with the products being assessed,
- They report to their CB any vulnerability they are aware of that affects the compliance of a certified ICT product with the certification requirements, in accordance with the provisions of the EUCC scheme,
- They support the CB, and upon request the NCCA, in the implementation of their compliance monitoring obligations and processes.

The ITSEF of a certified ICT product shall be involved by the NCCA in monitoring activities, where the NCCA deems it necessary.

The monitoring activity may under circumstances consist, among other things, in the re-assessment of the ICT product by the ITSEF upon request of the CB, accompanied - if necessary - by an audit subject to the monitoring activities (for example compliance of the complaints procedure, events of a security incident,…).

### 6.2.14 Patch management

EUCC, Article 13 Review of an EUCC certificate
EUCC, Annex IV.4 Patch management

Among the evaluation services related to ICT product certification that the ITSEF provides, patch management may be included upon request by the applicant. Patch management is associated to vulnerability handling and may also be used for the maintenance activities of certificates.

The ITSEF shall provide such services based on defined procedures and methods that ensure their conformity with the requirements laid out for ITSEFs in Annex IV.4 of the EUCC Regulation.

## 6.3 TRANSITION

ITSEFs that have applied to accreditation and for which the NAB has accepted the application should be allowed to engage into EUCC activities on evaluation projects before they are formally accredited.

The issuance of the final evalution technical report to the CB following successful performance of all evalution activities shall only be possible once the ITSEF has been accredited and where necessary authorized.

# ANNEX A TECHNOLOGY AND EVALUATION TECHNIQUE TYPES

This annex provides a taxonomy of technology and evaluation technique types, with examples. This taxonomy should be used both for the management of the competence of the ITSEF and for its assessment by NABs.

## A.1 TECHNOLOGY TYPES

### A.1.1 Hardware and software architectures, OS and applicative security

| Code | Description | Notes |
|---|---|---|
| S1 | Hardware architectures | Includes CPU architectures |
| S2 | Personal computer and server security | Includes general purpose operating systems |
| S3 | Embedded systems, microkernels | Includes trusted enviroments, realtime operating systems |
| S4 | Virtualization | |
| S5 | Applicative security | |
| S6 | Databases | |
| S7 | Web technologies | |

### A.1.2 Network & Wireless

| Code | Description | Notes |
|---|---|---|
| N1 | Network protocols | |
| N2 | Communication protocols | |
| N3 | Low-level interfaces | Includes serial line buses |
| N4 | Wireless | |
| N5 | Hardware components protocols | Includes hardware roots of trust |
| N6 | Phone and VoIP | |
| N7 | Mobile networks | Includes 3/4/5/6G |
| N8 | Filtering | |
| N9 | Intrusion detection | |

### A.1.3 Secure microcontrollers and smartcards

| Code | Description | Notes |
|---|---|---|
| H1 | Secure hardware components architectures | |
| H2 | Hardware sensors, reactive technology | |
| H3 | Platforms and applications security | Includes run-time systems, multiplatform interpreters/byte code execution environments |

### A.1.4 Cryptography

| Code | Description | Notes |
|---|---|---|
| C1 | State-of-the-art of Approved Cryptographic Mechanisms | |

## A.2 EVALUATION TECHNIQUE TYPES

The ITSEF is expected to indicate the reference to the definition of applied methods and the identification of tools used to exercise the evaluation techniques under assessment for accreditation.

Some references are included in the following tables, where alternative methods can be applied if proved equivalent by the ITSEF.

### A.2.1 Source code review

| Languages | Manual/automatic review | Reference to applied methods and/or tools (EUCC harmonized or ITSEF internal) |
|---|---|---|
| Example: C/C++ | Both | |

### A.2.2 Cryptographic analysis

| Object | Principle of the method | Reference to applied methods and/or tools (EUCC harmonized or ITSEF internal) |
|---|---|---|
| Cryptographic algorithms and protocols | Conformity analysis and tests | ISO/IEC 18367 Cryptographic algorithms and security mechanisms conformance testing |
| Random bit generators | Entropy analysis | ISO/IEC 20543 Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408 |
| Cryptographic protocols | Security assessment | ISO/IEC 29128 Verification of cryptographic protocols |

### A.2.3 Vulnerability analysis and penetration tests (generic)

| Technologies embedded in the evaluated product | Mastered attack technique | Reference to applied methods and/or tools (EUCC harmonized or ITSEF internal) |
|---|---|---|
| Fill-in using codes from Technology types. Example: S1, S2, N1 | Bypass<br>Code Injection<br>Denial of service<br>Direct attacks<br>Exploit development<br>Forensic analysis<br>Generational fuzzing<br>Generic vulnerability search<br>Hooking attacks<br>Memory dumps<br>Meta characters, encoding & input validation<br>Misuse<br>Mutational fuzzing<br>Overrun<br>Protocol attacks<br>Protocol fuzzing<br>Public exploits application<br>Race conditions<br>Tampering | ISO/IEC 20004 Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045<br>OWASP Penetration Testing Methodologies |

| Technologies embedded in the evaluated product | Mastered attack technique | Reference to applied methods and/or tools (EUCC harmonized or ITSEF internal) |
|---|---|---|
| | Web application security | |

### A.2.4 Vulnerability analysis and penetration tests (smartcards and similar devices)

| Technologies embedded in the evaluated product | Mastered attack technique | Reference to applied methods and/or tools (EUCC harmonized or ITSEF internal) |
|---|---|---|
| Fill-in using codes from Technology types. Example: H1, H2, H3 | Non-invasive /side channel attacks (electric consumption, electromagnetic radiations, execution time)<br>Semi-invasive simple attacks (light injection, electromagnetic injection, power/clock frequency glitch)<br>Invasive attacks: components preparation and probing | |

### A.2.5 Vulnerability analysis and penetration tests (hardware devices with security boxes)

| Technologies embedded in the evaluated product | Mastered attack technique | Reference to applied methods and/or tools (EUCC harmonized or ITSEF internal) |
|---|---|---|
| Fill-in using codes from Technology types. Example: H1, H2, H3 | Identification of components on a PCB<br>Debug interfaces manipulation (JTAG, UART)<br>Security boxes tampering<br>Disabling sensor networks<br>Non-invasive /side channel attacks (electric consumption, electromagnetic radiations, execution time) | |

# ANNEX B COLLECTION OF DEVELOPER EVIDENCE

This annex presents some of the alternatives that the developer may choose to present evidence for evaluation, and the ways in which the evaluator may respond while complying with the requirements of ISO/IEC 17025. It also identifies and considers cases where there may be a danger that evaluators undertake work that is strictly outside their accreditation scope.

## B1 BACKGROUND

The way the Common Criteria are phrased implies that the developer should supply specific documents containing each particular type of evidence. Normally it will be most efficient if that is the case; the effort required by the evaluator to review the evidence will thereby be minimised. However, there is no explicit requirement on the format of the evidence; only the information content is prescribed. In particular cases it may be more efficient for the developer to present the evidence in more diffuse form, which then requires more substantial evaluator effort to review. Provided that this can be done objectively and impartially, this support provided by the evaluator for collection of evidence could be considered completely acceptable.

The emphasis is on the objective justification of evaluation verdicts from developer-supplied deliverables. Where objective justification is not possible, the work becomes creation rather than collection of evidence. The aspect of creation is presented in this document only to help the reader in making the difference with collection. This document does not describe how creation of evidence could be used in an evaluation.

This document makes the distinction between two different ways permitting to obtain the evidence required by the Common Criteria:

- Documentation corresponding to classical approach: the developer delivers directly all the necessary information;
- Information: based on existing developer documentation and completed by additional information written in collection of evidence reports (e.g. filled questionnaire).

## B2 INTERPRETATION OF THE COMMON CRITERIA

The developer is responsible for providing the information required by the Common Criteria. The evaluator may collect some of this information provided that:

a) Evaluator contributions are fully endorsed by the developer

The information provided by the evaluator during collection process shall be accepted by the developer and integrated in the documentation configuration management of the TOE, i.e. registered as complementary evaluation evidence.

b) Approval is given in advance by the CB

Before beginning the project, ITSEF and developer shall agree on the tasks which could use this method. The agreement shall be officially communicated to the certification body during the evaluation registration, which permits to inform and get an approval by the CB of the approach chosen by the evaluation. The CB is already informed that the tasks which can be evaluated with the help of this method are ALC[3], ADV[4] and ATE[5]. Nevertheless, for each evaluation, the evaluator shall inform the CB of what type of documentation will be provided directly by the developer, and what information will be collected by the evaluator.

c) The evaluator contributions are independently reviewed by other members of the evaluation team, and their review is documented in the Evaluation Technical Report (ETR), or in intermediary evaluation reports.

Evaluation reports are already systematically reviewed, even in the classical approach, according to the standard ISO/IEC 17025. For the specific information produced by the developer during collection of evidence, attention of the

[3] Life-cycle support assurance class of the Common Criteria
[4] Development assurance class of the Common Criteria
[5] Tests assurance class of the Common Criteria

reviewer is particularly focused on the verification that no creation of evidence has been done by the evaluator (only collection of evidence).

## B2.1 Collection of evidence

The evidence to be provided by the developer may be presented in a single document that addresses all the requirements of an assurance component, or the evidence may need to be collected from a number of documents. Collecting evidence from a number of separate sources and formats is legitimate evaluator work. It may be convenient for the evaluator to construct a working document that approximates the ideal developer deliverable, but it is not mandatory. The evaluator work shall be limited to the objective collection of developer supplied material, rather than subjective creation, so that it remains repeatable, reproducible and impartial. A suitable test is whether any competent evaluator would obtain essentially the same result.

Objective collection of evidence is proper to the evaluators. It should not be considered as consultancy under the conditions expressed in this Annex, and therefore does not need to be performed by an independent team.

### B2.1.1 Determining when collection of evidence can be useful

The collection of evidence method as further defined in this chapter may be used by the evaluator to reduce iterations due to documentation changes. It is necessary to keep in mind that the method can permit to:

- Take into account developer practices (Fit the method with the practice) if the Common Criteria requirements can be covered;
- Take into account evaluation limited workload, without impacting evaluation assurance level.

A significant part of evaluation problems are due to documentation related iterations. That is to say, information is initially incomplete or inconsistent in documentation, even if the contents required by the assurance component can be finally verified after some documentation iterations. The goal of the method is to minimise these iterations on private/internal developer documents (it can not be applicable to the security target or the guidance documentation of the product).

The second goal of this method is to base as much as possible the evaluation work on real documentation used by the developer and not documentation written for Common Criteria purpose only. The evaluator will use the “Collection of Evidence” method to limit as much as possible some developer documentation written after the development.

Important note: the method targets documentation problems which do not cause a final evaluation FAIL verdict. Typically, a “documentation problem” issued by the evaluator permitting to conclude that a security functional requirement (SFR) is actually not implemented will not be solved by the “collection of evidence” method. This is the reason why the method guarantees the same evaluation level as the classical approach considering that the developer shall deliver directly all the information without the need for the evaluator to collect it.

Two different ways permit to obtain the evidence required by the Common Criteria and shall be considered depending on evaluation cases: documentation and information (documentation completed by evidence collected, such as a filled questionnaire).

### B2.1.2 Determining the scope of the collection of evidence for a specific evaluation

The developer and the evaluator shall first make an assessment of the existing developer documentation in relation with the evaluation tasks related to ADV, ALC, ATE. Some initial documentation shall be available to the evaluator in relation with these evaluation activities; otherwise, it is clear that some aspects of the evaluation will not be covered. The level of information provided shall give the evaluator and CB sufficient trust that the evaluation could succeed with a positive result.

This assessment shall take into account the targeted evaluation assurance level. Once this initial assessment is done, the evaluator concludes whether the targeted scope for collection of evidence usage is a priori acceptable, and informs the CB of what type of documentation will be provided directly by the developer (corresponding to which evaluation activities or parts of), and what information will be collected by the evaluator. The CB will be then able to approve or not the scope of collection of evidence usage.

The evaluation verdict finally guarantees the sufficiency of the initial set of documents delivered. Indeed, it results that the information which shall be directly provided by the developer (for strict conformance to the Common Criteria or for efficient understanding by the evaluator) has actually been provided; otherwise the evaluation verdict will be FAIL.

### B2.1.3 Preliminary activity: Training on product

This step is not strictly speaking part of the collection of evidence methodology. Nevertheless, it can be a benefit for the evaluator to quickly understand the context of the product environment and the context of the evaluation. Thus, the evaluator can take advantage of this training to determine whether he will be able to collect evidence during the evaluation. It also permits to understand the target of evaluation (TOE) scope compared to the product.

This training shall permit the evaluator to:

- Improve the security target (ST) evaluation relevance;
- Gain a functional knowledge of the TOE before starting FSP[6] and guidance evaluation.

During this training, the evaluator shall obtain:

- A description of the ST by the ST writer;
- A TOE security function interfaces (TSFI) description, but also a description of the other product interfaces which are not considered as “TSFI”;
- A description of the tools supporting communication with the TOE. The developer shall deliver these tools to the evaluator;
- Access to design information to be able to understand the product overall architecture (for TDS[7] evaluation activities).

In case the evaluator would conclude at the end of this initial training that the developer’s input and the status of the documentation is not suitable or sufficient for ‘collection of evidence’, he would conclude that ‘collection of evidence’ is not feasible for the product under consideration. Consequently, the classical approach of the CEM would be preferred for the evaluation.

### B2.1.4 The collection of evidence in practice

Some assurance components can not be concerned by the collection of evidence:

- ASE[8]_xxx/APE[9]_xxx: the Security Target/Protection Profile is a document being a basis for the whole evaluation, which will be often public. This document shall be complete and coherent as the evaluator will base the understanding of the evaluation on it.
- AGD[10]_xxx: Guidance documentation constitutes part of the TOE delivered to the users. Deficiencies therefore constitute errors. It is not permissible for the evaluator to make up for deficiencies.
- Work units of components that involve semi formal/formal method: semi formal and formal approaches are basically difficult to associate with incomplete documentation necessitating collection of evidence. Nevertheless, the collection of evidence can be used for parts of these components. For instance, a questionnaire can be used to understand the formal method used. But it will not be applicable to the formal model itself.

Due to the fact that the evaluator shall not create but rather collect evidence, the information provided by the evaluator will mainly have the form of a questionnaire constructed with open-ended questions that do not suggest the required answer. Indeed, the form of the questionnaire permits to focus the collection on the information actually required by the evaluator, corresponding to the information missing in the existing documentation (a preliminary work from the evaluator is necessary to determine which information is missing and to prepare the corresponding questions).

The evaluator shall make a clear difference between the information directly collected (i.e. the answers given by the developer) and his own analysis/comments directly linked to these answers. Indeed, as the same document can

[6] Functional specification assurance family of the Common Criteria
[7] TOE design assurance family of the Common Criteria
[8] Security target evaluation assurance class of the Common Criteria
[9] Protection Profile evaluation assurance class of the Common Criteria
[10] Guidance documents assurance class of the Common Criteria

include both developer answers and evaluator analysis, it is fundamental to make a clear distinction between them. For example, if the questionnaire has the form of a table, the difference can be marked thanks to separate rows or columns developer answer/evaluator comment.

The CB will be informed when the interviews sessions occur and can decide to attend the sessions.

### B2.1.5 Evaluator contributions are finally endorsed by the developer

Once evidence has been completely collected, the evaluator delivers it to the CB and to the developer. The developer shall appropriate the information collected as it become complementary evaluation evidence. This evidence shall be included in the configuration management system of the TOE

The developer can decide to integrate the information collected directly in its own documentation to improve it for further evaluations and make easier reuse of it, but it is not required by the methodology.

## B2.2 Creation of evidence compared to Collection of evidence

The difference between objective collection and subjective creation of evidence is illustrated by considering the difference between an open-ended and a leading question to the developer. If the evaluator would make a definite hypothesis and would ask the developer for a yes or no confirmation, this falls on the side of creation of evidence, but an open-ended question that does not suggest the required answer falls on the side of collection of evidence.

A typical question corresponding to creation of evidence could be: “can you confirm that this SFR is implemented in this part of the design?”. Since the intention of the criteria is that developers should demonstrate familiarity with the IT features of the TOE, and that they have taken care with the security aspects, developer shall be able to answer to open questions corresponding to collection of evidence. The question corresponding to collection of evidence would be: “Can you indicate the part of the design where this SFR is implemented?”

The leading questions which are corresponding to creation of evidence are related to information directly linked to the evaluation criteria and to the verdict of the evaluation activity, such as leading questions related to design information, implementation of security measures in development environment, etc.

## B2.3 Small deficiencies

The evaluator may address small deficiencies in a developer-supplied deliverable by interviewing the developer and documenting his response, or by making hypotheses and requesting developer confirmation; however the evaluator should check the consistency of such input with other developer-supplied material. When doing so, the evaluator must supply a rationale, to be agreed by the Certifier, that the compensatory work is not excessive. Typically, the information and the rationale can be directly added in the evaluation report.

These small deficiencies shall be limited to some information such as careless mistakes, lack in a reference to a documentation which can be easily confirmed, etc. The difference with creation of evidence is the importance of information to be confirmed by the developer in relation with the criteria: the small deficiencies shall correspond to any incompleteness/inconsistency which does not have an impact on the verdict for the corresponding evaluation activity.

## B2.4 Examples of information which can be collected

The requirement for the developer to provide correspondence analysis does not necessarily demand the production of a tabular summary. If traceability is evident the evaluator may produce such a summary (if required) as part of the collection of evidence. On the other hand, if correspondences have to be inferred based on general similarities of the functions involved, then the work goes outside the scope of collection and correspond to creation of evidence.

The design supplied by the developer may be found to be incomplete in certain respects, for example it may not provide complete details of all modules. There is scope for evaluator collection of supplementary evidence from alternative sources, such as:

a) Other relevant design information.

This may include design documents for closely related TOEs, standard texts (e.g. on Unix or NT internals), as well as documentation relevant to the targeted version of the TOE which may provide a useful context (e.g. the functional specification).

b) Evidence in ETRs from previous evaluations of the TOE (i.e. involving an earlier version or a different variant).

Where the evaluators in a previous evaluation of the TOE have documented in detail their understanding of the internal workings of the TOE security, such evidence may assist the evaluators in gaining the required overall understanding of the internal workings of the TOE.

c) Developer presentations of particular aspects of the TOE security.

Developer presentations may help the evaluators to gain an overall understanding of particular parts of the TOE, for example how certain TOE security functions are implemented, or an overview of the internal workings of individual TOE subsystems. Such evidence may be used to complete the low-level design. Any information presented verbally which represents piece of evidence shall be documented by the evaluators and, any such input should be checked for consistency with other developer-supplied evidence.

d) Clarifications of specific technical queries from the evaluators, whether verbal or written (e.g. email).

Such evidence should be used to confirm the evaluator's understanding of specific points of technical detail.

e) Evidence generated by the developer's configuration management system.

Such evidence may be useful in helping to establish an accurate picture of the interrelationships between modules, e.g. call trees (identifying which modules depend on which other modules), use of global data structures by modules, and so on.

f) Module headers associated with the source code modules.

This will typically take the form of design evidence contained within comments in the source code modules or header files.

g) The source code itself, including any associated comments.

It is not anticipated that it would be practical to derive any substantial proportion of the detailed design from the source code itself, but it may be used to address particular questions of details, as comments within the source code may be.

## 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