EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUCC SCHEME

STATE-OF-THE-ART DOCUMENT

ACCREDITATION OF ITSEFs FOR THE EUCC SCHEME

Version 1.6c, November 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 linking to the SOG-IS document, which the state-of-the-art document is based on Rephrasing of subcontracting and non-compliance conditions Addition of cryptography in the Annex	Based on comments received
October 2023	1.1		Endorsed for publication on 20 October 2023 by the ECCG and adopted by the European Commission via comitology procedure on 31 January 2024
April 2024	1.2	Clarification of requirements on independence and consultancy	Version submitted to the ECCG for comments
29 April 2024	1.3	New clarification of requirements on independence and consultancy Addition of a transition chapter	Update based on the latest ECCG comments received after the ECCG meeting of 15 April 2024 Version submitted to the EA
30 April 2024	1.4	Deletion of the EA table Additional clarification of requirements on independence and consultancy, including the EUCC related examples	Update based on the EAs input Version submitted to the ECCG for comments
23 May 2024	1.5	Alignment of the legal information and the introduction with the SoA document on the accreditation of CBs to the EUCC scheme Additional clarification of the requirements on independence and consultancy Clarification of the scope of the accreditation Addition of Annex B on 'Collection of developer evidence' according to the equivalent SOG-IS document	Update based on the EA, the ECCG and CABs input Version submitted to the ECCG and the EA for comments
4 June 2024	1.6a	Clarification of the scope of the accreditation (Chapter 5) Clarification of the independence requirement (Chapter 6.2.1) Minor correction of the title of Annex A2.2 Correction of typos	Update based on the EA and the ECCG for comments Version submitted to the ECCG for endorsement
21 June 2024	1.6b	Minor correction in the table in Chapter 6.1 Deletion of the standards reference dates Re-clarification of the independence requirement (Chapter 6.2.1)	Version submitted to the ECCG for endorsement Endorsed for publication on 05/07/2024 by the ECCG

		Transposition of the references to the EUCC candidate scheme to references to the EUCC Implementing Regulation	
31 July 2024 – 15 November 2024	1.6c	Editorial changes Clarification of transition rules	Changes following the review by the European Commission and during the comitology procedure

LEGAL INFORMATION

LEGAL NOTICE

This document needs to be read together with Regulation (EU) 2019/881, Commission Implementing Regulation (EU) 2024/482, including its annexes, potential updates of the Implementing Regulation, and where applicable supporting documentation that is made available.

The document should be updated in line with latest developments and best practices in accreditation. Updates to this document should be submitted to the European Cybersecurity Certification Group (ECCG) for endorsement.

This document is accessible to the public 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 of the maintenance of the scheme is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

CONTACT

Contact to provide constructive feedback or questions related to this publication can be found on Cybersecurity Certification (europa.eu)[1].

[1] https://certification.enisa.europa.eu/

TABLE OF CONTENTS

1 INTRODUCTION 6

1.1 RESPONSIBILITIES OF THE NATIONAL ACCREDITATION BODY 6

1.2 RESPONSIBILITIES OF THE NATIONAL CYBERSECURITY CERTIFICATION AUTHORITY 6

2 NORMATIVE REFERENCES 7

3 ACRONYMS AND DEFINITIONS 8

3.1 ACRONYMS 8

3.2 DEFINITIONS 9

4 APPLICABILITY OF INTERNATIONAL STANDARDS TO THE ACCREDITATION OF ITSEFS 10

5 SCOPE OF ITSEF ACCREDITATION 10

6 ACCREDITATION REQUIREMENTS 11

6.1 GENERAL ACCREDITATION REQUIREMENTS FROM THE CSA 11

6.2 SPECIFIC ACCREDITATION REQUIREMENTS 15

6.2.1 Independence 15
6.2.2 Impartiality 15
6.2.3 Confidentiality 16
6.2.4 Competence 17
6.2.5 Facilities 18
6.2.6 Subcontracting 18
6.2.7 Non-compliance 18
6.2.8 Retention of records 19
6.2.9 Ensuring the validity of results 19
6.2.10 Management system documentation 19
6.2.11 Quality process 19
6.2.12 Composite evaluations 19
6.2.13 Monitoring compliance 20
6.2.14 Patch management 20

6.3 TRANSITION 20

ANNEX A TECHNOLOGY AND EVALUATION TECHNIQUE TYPES 21

A.1 TECHNOLOGY TYPES 21

A.1.1 Hardware and software architectures, operating systems and application security 21
A.1.2 Network & wireless 21
A.1.3 Secure microcontrollers and smartcards 21
A.1.4 Cryptography 21

A.2 EVALUATION TECHNIQUE TYPES 21

A.2.1 Source code review 22
A.2.2 Cryptographic analysis 22
A.2.3 Vulnerability analysis and penetration tests (generic) 22
A.2.4 Vulnerability analysis and penetration tests (smartcards and similar devices) 23

A.2.5 Vulnerability analysis and penetration tests (hardware devices with security boxes) 23

ANNEX B COLLECTION OF DEVELOPER EVIDENCE 24

B1 BACKGROUND 24

B2 INTERPRETATION OF THE COMMON CRITERIA 24

B2.1 Collection of evidence 25
B2.1.1 Determining when collection of evidence can be useful 25
B2.1.2 Determining the scope to collect evidence for a specific evaluation 25
B2.1.3 Preliminary activity: training on product 26
B2.1.4 The collection of evidence in practice 26
B2.1.5 Evaluator contributions endorsed by the developer 27
B2.2 Creation of evidence compared to collection of evidence 27
B2.3 Minor deficiencies 27
B2.4 Examples of information which can be collected 27

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 on the accreditation of Information Technology Security Evaluation Facility (ITSEFs), as defined in the EUCC scheme, that establishes they are technically competent for their related tasks under the Common Criteria and the Common Evaluation Methodology.

This technical competence needs to be assessed through the accreditation of the ITSEFs by a National Accreditation Body (NAB) in line with EN ISO/IEC 17025:2017 in accordance with point 20 of Annex of the Cybersecurity Act.

As EN ISO/IEC 17025:2017 applies to a very general and wide range of testing activities, this document interprets the standard and the EUCC specific requirements for ITSEFs whose conformity is to be assessed during their accreditation.

This document must be used by the National Accreditation Bodies (NABs) to support their compliance assessments in accordance with the EUCC.

1.1 RESPONSIBILITIES OF THE NATIONAL ACCREDITATION BODY

The NAB, that is established in a Member State in line with Regulation (EC) 765/2008, is responsible for performing the accreditation for a conformity assessment body (the Certification Body (CB) and the ITSEF. Both of these 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 efforts by using the work that was carried out during the accreditation process as much as possible in the authorisation 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. The TAs and TEs used by the NAB must however operate under the sole responsibility of the NAB for their accreditation activities.

In addition, the NAB needs to perform the following tasks:

- report the results of the accreditation assessment to the NCCA, including assessment reports and decisions for granting, extending, reducing, suspending, or withdrawing the accreditations for EUCC;
- apply an assessment programme to assess that the accredited conformity assessment bodies meet the accreditation requirements;
- 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 event of infringements of the CSA, in particular on the requirements of Annex to the CSA, the collaboration with the NCCA is an important factor since the NCCA has monitoring and supervisory 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 taken by the NAB, the NCCA must notify the European Commission in accordance with Article 61 CSA and relevant implementing regulation[2].

ENISA will make the information regarding the notified conformity assessment bodies available on its dedicated website on European cybersecurity certification schemes referred to in Article 50(1) of Regulation (EU) 2019/881.

The monitoring and supervisory national cybersecurity certification authorities (NCCAs) are responsible for: (i) actively assisting and supporting the NAB in their monitoring and supervising tasks; and (ii) sharing information and reporting to the NAB. This cannot obstructa the handling of complaints performed by the ITSEF in line with EN ISO/IEC 17025:2017 concerning any:

[2] Implementing Regulation …/…. establishing the circumstances, formats and procedures for notifications pursuant to Article 61(5) of Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification

- (potential) non-compliance of the ITSEF related to the accreditation requirements annexes in Regulation (EU) 2029/881 (Cybersecurity Act- Article 58(7), point (c) and Article 58(7), points (h) and (i) CSA);
- complaints received related to the authorisation of an 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 for the monitoring and supervision of the CABs (CBs & ITSEFs), in line with Article 58 (7)(g) Regulation (EU) 2019/881 in an annual summary report and send this to the ECCG and the ENISA.

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)[3].

ISO/IEC 15408-1:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model.

ISO/IEC 15408-2:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 2: Security functional components.

ISO/IEC 15408-3:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 3: Security assurance components.

ISO/IEC 15408-4:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 4: Framework for the specification of evaluation methods and activities

ISO/IEC 15408-5:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 5: Pre-defined packages of security requirements.

ISO/IEC 18045:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation.

EN ISO/IEC 17025:2017 - General requirements for the competence of testing and calibration laboratories.

EN ISO/IEC 17065:2012 - Conformity assessment - Requirements for bodies certifying products, processes and services.

ISO/IEC 19896-1:2018 - IT security techniques - Competence requirements for information security testers and evaluators - Part 1: Introduction, concepts and general requirements.

[3] Available at : http://data.europa.eu/eli/reg_impl/2024/482/oj

ISO/IEC 19896-3:2018 - 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 23532-1:2021 - 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 ACRONYMS

CAB	Conformity assessment body
CB	Certification body
CC	Common Criteria for Information Technology Security Evaluation as defined in the EUCC
CEM	Common Methodology for Information Technology Security Evaluation as defined in the EUCC
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 Organisation for Standardisation
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 (CSA) and under Article 2 of the Implementing Regulation (EU) 2024/482 apply to this document. The following definitions also apply to this document.

Conformity Assessment Body
In line with Article 2 of Regulation (EU) 2019/881,'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
In accordance with Regulation 2024/482, '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 the EUCC.

Evaluation
'Evaluation' means an assessment of the applicant's claimed Security Functional 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 (EN ISO/IEC 17065:2012).

Evaluation tasks can include activities such as design and documentation review, sampling, testing, inspection and audit (EN ISO/IEC 17065:2012).

In the context of the EUCC, an evaluation can be defined as the 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
In accordance with Regulation 2024/482, '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 (EN ISO/IEC 17025:2017).

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

The ITSEF can be a body that together with the CB forms a single 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 must 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 EN ISO/IEC 17025:2017 and the CB needs to meet the requirements of standard EN ISO/IEC 17065:2012.

Evaluator
'Evaluator' means ITSEF personnel performing evaluation activities.

4 APPLICABILITY OF INTERNATIONAL STANDARDS TO THE ACCREDITATION OF ITSEFS

The CSA requires 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, the following standards must apply to the accreditation of ITSEFs:

- EN ISO/IEC 17025:2017 - General requirements for the competence of testing and calibration laboratories: meeting this standard is mandatory for ITSEF accreditation.

Furthermore, the following standards should be considered to be applied:

- ISO/IEC TS 23532-1:2021 - 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 interprets EN ISO/IEC 17025:2017 which also applies to the ITSEF accreditation.

Note: ISO/IEC TS 23532-1:2021 references to 'scheme owner(s)' should be understood in this context as referring to the related accredited and, if applicable authorised CB and NCCA.

- Additions to some ISO/IEC TS 23532-1:2021 requirements are defined in this document, that should be considered for ITSEF accreditation.
- Additional competence requirements are defined in this document, based on ISO/IEC 19896:2018 - IT security techniques - Competence requirements for information security testers and evaluators, both parts 1 and 3, that define the elements of competence, competency levels and the measurement of the elements of competence, that are to be applied by ITSEFs.

Note: ISO/IEC 19896:2018 includes 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 (see Chapter 6.2.4 'Accreditation requirements'.

The 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 EN ISO/IEC 17025:2017 accreditation for EUCC ITSEFs must be based on the following standards:

- the CC standard;
- the CEM standard.

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

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

Only the information described as 'Type of test and test parameter' can 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 line with the applicable standards and the requirements defined under the Annex of the CSA.

The scope of accreditation must 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 assurance components of ISO/IEC 15408-3:2022 in which the ITSEF has proven technical competence to evaluate in line with ISO/IEC 18045:2022, for example:
  - IT security evaluation up to EAL 3 augmented with ALC_FLR.2
- The reference to the scheme:
  - EUCC.

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

6 ACCREDITATION REQUIREMENTS

The following EUCC scheme ITSEF accreditation requirements must apply:

- The requirements for the competence of testing and calibration laboratories as defined in EN ISO/IEC 17025:2017 The requirements as defined in ISO/IEC TS 23532-1:2021 should be considered.
- Those requirements that are to be met by conformity assessment bodies as set out in the Annex to the CSA, where they apply to the ITSEF activities (see Section 6.1 'General accreditation requirements from the CSA').
- The requirements set out in this document (see Section 6.2 'Specific accreditation requirements', based on those requirements applicable to ITSEFs indicated in the EUCC - except those related to authorisation.

6.1 GENERAL ACCREDITATION REQUIREMENTS FROM THE CSA

Conformity assessment bodies that wish to be accredited must meet the requirements set out in the Annex to the CSA (see Table below). Bearing in mind that the ITSEF's role is to evaluate and not to certify the ICT products, the table below shows to which extent the requirements apply to the ITSEF. It also provides links to related requirements under EN ISO/IEC 17025:2017 that may support compliance to the indicated CSA requirements in the second column of the table.

Requirements from the CSA Annex 'REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES'		Supporting EN ISO/IEC 17025:2017 requirement
1.	A conformity assessment body shall be established under national law and shall have legal personality.	EN ISO/IEC 17025:2017, 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.	EN ISO/IEC 17025:2017, 4.1 Independence
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.	EN ISO/IEC 17025:2017, 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.	EN ISO/IEC 17025:2017, 4.1 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.	EN ISO/IEC 17025:2017, 4.1 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.	EN ISO/IEC 17025:2017, 4.1 EN ISO/IEC 17025:2017, 4.2 EN ISO/IEC 17025:2017, 6.6.2 Impartiality Confidentiality

Requirements from the CSA Annex 'REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES'		Supporting EN ISO/IEC 17025:2017 requirement
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.	EN ISO/IEC 17025:2017, 4.1 Impartiality EN ISO/IEC 17025:2017, 6.2.3 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.	EN ISO/IEC 17025:2017, 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:	EN ISO/IEC 17025:2017, 6.2 EN ISO/IEC 17025:2017, 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.	EN ISO/IEC 17025:2017, 6.3 EN ISO/IEC 17025:2017, 6.4
12.	The persons responsible for carrying out conformity assessment activities shall have the following:	EN ISO/IEC 17025:2017, 6.2
(a)	sound technical and vocational training covering all conformity assessment activities;	Competence

Requirements from the CSA Annex 'REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES'		Supporting EN ISO/IEC 17025:2017 requirement
(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.	EN ISO/IEC 17025:2017, 4.1 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.	EN ISO/IEC 17025:2017, 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.	EN ISO/IEC 17025:2017 4.2 EN ISO/IEC TS 23532-1:2021 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 performing certification of ICT products, ICT services or ICT processes.	This point does not apply to ITSEFs, see point 20.

Requirements from the CSA Annex 'REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES'	Supporting EN ISO/IEC 17025:2017 requirement
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.	EN ISO/IEC 17025:2017

6.2 SPECIFIC ACCREDITATION REQUIREMENTS

In addition to the requirements included in EN ISO/IEC 17025:2017 and ISO/IEC TS 23532-1:2021, the following requirements apply to the accreditation of an EUCC ITSEF.

6.2.1 Independence

The independence criteria set out in CSA Annex point 2 must be applied to the ITSEF, but not to the entire legal entity (if the ITSEF is part of a bigger legal entity). It must also apply to the ICT product, ICT process, ICT service under evaluation.

The ITSEF must 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 under EN ISO/IEC 17025:2017 to its clients.

This does not preclude:

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

The ITSEF must 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

EN ISO/IEC 17025:2017, '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 17025:2017 on impartiality. In addition, 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)[4] of the ITSEF must not be considered as 'consultancy'.

a) Preparation of evaluation documentation and evidence in line 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 must exclude recommendations regarding the implementation of a specific architecture or mechanism.

[4] The policy agreed by EA Members for relationship between conformity assessment bodies and consultancy activities, available at https://european-accreditation.org/?s=ea-2%2F20.

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

d) Participation in R&D projects, studies and to the maintenance of the EUCC scheme related to or encompassing 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), on condition that:
   - the ITSEF allows 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, on condition that:
   - the ITSEF establishes an analysis before project launch to check there is no impact on conformity assessment or on assessed parties which might be competitors;
   - the activity relates to the complete sector, and must neither be for the ITSEF nor for an individual industrial, and the ITSEF must provide collective and transparent communication;
   - there must not be subsequent certification of an ICT product related to a patent;
   - there must not be any user licence resulting in collective certification.

f) Delivery of a service that could be a conformity assessment but is outside of the scope of the accreditation for the 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), on condition that:
   - the validation of the method meets the EN ISO/IEC 17025:2017 requirements;
   - the ITSEF provides a generic test or inspection protocol and makes it publicly available; or
   - the ITSEF only provides a specific test or inspection protocol that is not publicly available for the benefit of evaluation and certification activities outside the scope of the accreditation.

Where an activity is considered as acceptable with conditions, the ITSEF must meet the conditions and provide detailed proof of this to the NAB.

6.2.3 Confidentiality

EUCC, Recital 27 & Article 43 Protection of information
EN ISO/IEC 17025:2017, '4.2 Confidentiality'

Additional requirement to **ISO/IEC TS 23532-1:2021**, 4.2.6

It should be considered for the exclusions set out in ISO/IEC TS 23532-1:2021, 4.2.6 to be noted and justified in the ETR to the competent CB. If the responsible CB considers that access to this information is relevant to performing the certification decision, it can be a reason for rejecting the requested certificate.

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

Additional requirement to **ISO/IEC TS 23532-1:2021**, 4.2.8

The scope of the policies, procedures and security manual to ensure the protection of proprietary information must 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 authorities and bodies concerned;
- 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 must 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, must be sufficiently 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 must 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 of 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 must also cover the following measures:

a) the information system must include tools that provide encryption functions for non-public information at rest. These tools should be referenced by an ENISA or a national guidance document.
Encryption tools that are deployed to secure information are expected to comply with, by order of precedence:
   - EU and national laws on the protection of sensitive information;
   - recommendations, guidance and opinions from the Member State's competent cybersecurity authorities;
   - recommendations from the ECCG.

b) For non-public information, secure electronic storage and communication must be achieved through accepted and recognised cryptographic methods and algorithms. The ITSEF must refer to and comply with ENISA or national cryptography guidelines for further guidance.

c) ITSEF staff must be trained on handling information and sign agreements on compliance with information security obligations to maintain data secrecy. The ITSEF must store these agreements in line with the requirements on the retention of records.
All staff must sign an non-disclosure agreement (NDA) before being granted access to non-public information. In governmental organisations where there are binding legal rules on information secrecy, these rules must take precedence, unless they interfere with EU law.
The ITSEF must maintain a updated information security workshop schedule for staff involved in the EUCC scheme process. The workshop must take place on a regular basis and include updates on relevant regulatory changes.

Evaluation contracts between ITSEFs and their customers must 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. Where necessary, the CB and the NAB for the purpose of accreditation, and the NCCA for the purpose of its monitoring and supervision tasks, must be informed about these contractual obligations.

6.2.4 Competence

EUCC, Recital 19 & Article 23 Notification of certification bodies
EN ISO/IEC 17025:2017, '6.2 Personnel'

The ITSEF, their evaluators and, if applicable, the relevant staff of their subcontracted parties must 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 must define and operate a competence management system for the evaluators and must demonstrate a appropriate level of competence, expertise and knowledge. It is strongly recommended to demonstrate that:

- the elements of competence, competency levels and the measurement of the elements of competence are drawn from ISO/IEC 19896-1:2018, or if they differ, are commensurate with the objectives that are defined and at least be equivalent to the elements under ISO/IEC 19896-1:2018;
- the knowledge, skills, experience and education, and the applicable requirements for the evaluators are drawn from ISO/IEC 19896-3:2018, or if they differ, are commensurate with the objectives and be at least equivalent to the requirements under ISO/IEC 19896-3:2018;
- the knowledge required for evaluating security assurance requirement classes is based on Annex B of ISO/IEC 19896-3:2018;
- the knowledge required for evaluating security functional requirement classes is based on Annex C of ISO/IEC 19896-3:2018;
- the knowledge required for evaluating specific technologies and exercising different evaluation technique types are specified by the ITSEF using the classification provided in the Annex A.
  The ITSEF may use other classification criteria, as long as it can be mapped to the one provided in the Annex A. The mapping and the supporting rationale must 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
EN ISO/IEC 17025:2017, '6.3 Facilities and environmental conditions'

Additional requirement to **ISO/IEC TS 23532-1:2021**, 6.3.1.1

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

6.2.6 Subcontracting

EN ISO/IEC 17025:2017, '6.6 Externally provided products and services'

The ITSEF must 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 subcontracted third-party must 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 subcontracting, the evaluator must be present and instruct the equipment operating staff. To instruct the operating staff, evaluators must 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 must support the CBs, for which it performed evaluation activities, in their handling of non-compliance 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
EN ISO/IEC 17025:2017, '7.5 Technical records', '8.4 Control of records'

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

All records must be securely and accessibly stored for at least 5 years after the expiry of the certificate, except if the records concern running investigations related non-compliance and complaint handling and their respective legal remedy procedures.

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

If a different period of validity has been attributed to a certificate in line with the conditions of the EUCC, Section II it must be taken into account when calculating the new retention period for the records.

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

6.2.9 Ensuring the validity of results

EN ISO/IEC 17025:2017, '7.7.2 Monitoring of laboratory performance'

This section requires that a laboratory must monitor its performance by comparing itself with the results of other laboratories. In particular, the ITSEF needs to show that it has a plan and where benchmarking has already been carried out, proof of participation and a report on the results can be provided.

6.2.10 Management system documentation

EN ISO/IEC 17025:2017, '8.2 Management system documentation (Option A)'

Additional requirement to **ISO/IEC TS 23532-1:2021**, 8.2.8

Evaluation procedures should be detailed enough to allow a technical competent evaluator to perform the evaluation without further guidance.

6.2.11 Quality process

EUCC, '11. RULES FOR MONITORING COMPLIANCE'
EN ISO/IEC 17025:2017, '8.8 Internal audits'

The ITSEF management process must comply with all the EUCC's applicable requirements and obligations, including the requirements for handling complaints.

6.2.12 Composite evaluations

EUCC, Article 7 Evaluation criteria and methods for ICT products

The ITSEF must operate within the defined procedures to ensure that, where an ICT product undergoes a composite product evaluation, necessary sensitive information to be reused from the initial evaluation is provided to the ITSEF performing the composite evaluation. This information must be shared through an ETR for composite evaluation, based on the template provided by ENISA.

The information sharing for composite evaluations must take place in full cooperation with the CBs, including the CB that has certified the base component and the CB handling the composite evaluation.

Besides the relevant documentation that should be shared, there must be a communication channel between all involved to clarify any technical problems. All parties/bodies, in particular 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 must have procedures and processes in place to show their continued compliance with the specified cybersecurity requirements under their certification.

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

To support compliance monitoring, ITSEFs must define a set of compliance monitoring processes to 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;
- systematically carry out a search for publicly known vulnerabilities in connection with the products being assessed;
- report to their CB any vulnerability they are aware of that affects the compliance of a certified ICT product with the certification requirements, in line with the EUCC scheme;
- 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 must be involved by the NCCA in monitoring activities, where the NCCA deems it necessary.

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

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 managing vulnerability and may also be used for the maintenance activities of certificates.

The ITSEF must provide such services based on defined methods and procedures to ensure their compliance with the requirements set out in Annex IV.4 to the EUCC Regulation.

6.3 TRANSITION

In the context of an accreditation process, ITSEFs may engage, under the supervision of the NAB and where necessary of the NCCA, into the required evaluation activities that should be assessed by the NAB, and, where necessary, by the NCCA.

However, the issuance of the final ETR to the CB upon successful completion of all evaluation activities requires that the ITSEF has been accredited and if necessary authorised., in accordance with Regulation (EU) 2019/881 and the EUCC.

The applicant and all parties involved in these activities must be fully aware of their status and accept the risks associated with the possibility that the ITSEF may not ultimately be accredited and, if necessary, authorised.

ANNEX A TECHNOLOGY AND EVALUATION TECHNIQUE TYPES

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

A.1 TECHNOLOGY TYPES

A.1.1 Hardware and software architectures, operating systems and application 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 environments, real time operating systems
S4	Virtualisation	
S5	Application 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 approved cryptographic mechanisms	

A.2 EVALUATION TECHNIQUE TYPES

The ITSEF should 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 accepted as equivalent by the ITSEF.

A.2.1 Source code review

Languages	Manual / automatic review	Reference to applied methods and/or tools (EUCC harmonised 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 harmonised or ITSEF internal)
Cryptographic algorithms and protocols	Conformity analysis and tests	ISO/IEC 18367:2016 Cryptographic algorithms and security mechanisms conformance testing
Random bit generators	Entropy analysis	ISO/IEC 20543:2019 Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408
Cryptographic protocols	Security assessment	ISO/IEC 29128-1:2023 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 harmonised or ITSEF internal)
Fill-in using codes from Technology types. Example: S1, S2, N1	Bypass	ISO/IEC 20004:2015 Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045 OWASP Penetration testing methodologies
	Code injection	
	Denial of service	
	Direct attacks	
	Exploit development	
	Forensic analysis	
	Generational fuzzing	
	Generic vulnerability search	
	Hooking attacks	
	Memory dumps	
	Meta characters, encoding & input validation	
	Misuse	
	Mutational fuzzing	
	Overrun	
	Protocol attacks	
	Protocol fuzzing	

Technologies embedded in the evaluated product	Mastered attack technique	Reference to applied methods and/or tools (EUCC harmonised or ITSEF internal)
	Public exploits application Race conditions Tampering 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 harmonised 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)	
	Semi-invasive simple attacks (light injection, electromagnetic injection, power/clock frequency glitch)	
	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 harmonised or ITSEF internal)
Fill-in using codes from Technology types. Example: H1, H2, H3	Identification of components on a PCB	
	Debug interfaces manipulation (JTAG, UART)	
	Security boxes tampering	
	Disabling sensor networks	
	Non-invasive / side channel attacks (electric consumption, electromagnetic radiations, execution time)	

ANNEX B COLLECTION OF DEVELOPER EVIDENCE

Annex B presents some of the alternatives that the developer may use to present evidence for evaluation, and the ways in which the evaluator may respond while complying with the requirements of EN ISO/IEC 17025:2017. It also identifies and considers cases where there may be a risk that evaluators undertake work that is outside the scope of their accreditation.

B1 BACKGROUND

The Common Criteria require different types of evidence to be presented in specific documents made available by the developer to the evaluator. This way the burden on the evaluator to review the evidence is reduced. However, there is no explicit requirement on the format of the evidence; only the information that it needs to contain. In particular cases, it may be more efficient for the developer to present the evidence in different forms, which then requires more effort by the evaluator to review it.

Provided that this can be done objectively and impartially, the support provided by the evaluator to collect evidence could be considered as completely acceptable. Developer-supplied deliverables should allow the objective justification of evaluation verdicts by the evaluator. 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 to make the difference with the collection of evidence. This document does not describe how the creation of evidence could be used in an evaluation.

This document makes the distinction between two different ways of obtaining the evidence required by the Common Criteria.

- Documentation corresponding to the classical approach: the developer delivers 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 if the:

a) **evaluator contributions are fully endorsed by the developer** (the information provided by the evaluator during collection process must 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 the developer must agree on the tasks which could use this method. The agreement must 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[5], ADV[6] and ATE[7]. However, for each evaluation, the evaluator must 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 ETR or in the intermediary evaluation reports** (evaluation reports are already systematically reviewed, even in the classical approach, according to the standard EN ISO/IEC 17025:2017. For the specific information produced by the developer during collection of evidence, attention of the reviewer is particularly focused on the verification that no creation of evidence has been done by the evaluator (only collection of evidence)).

[5] Life-cycle support assurance class of the Common Criteria.
[6] Development assurance class of the Common Criteria.
[7] Tests assurance class of the Common Criteria.

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. The evidence may also need to be collected from a number of documents. Collecting evidence from a number of separate sources and formats is a legitimate part of the evaluator's work. It may be convenient for the evaluator to put together a working document that helps to deliver the job at hand, but it is not mandatory. The evaluator's work must 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 the same result.

Objective collection of evidence needs to be carried out by the evaluators. It should not be considered as the job of a consultancy under the conditions set out in Annex B, 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 method for the evidence, as further defined in this chapter, may be used by the evaluator to reduce iterations of evaluation activities due to documentation changes. The method allows the evaluator to take into account:

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

A significant part of the evaluation problems is due to updates of documents. That is to say, information is initially incomplete or inconsistent in documentation, even if the content required by the assurance component can be checked at the end.

The first goal of the method is to minimise these updates of private/internal developer documents (it does not apply to the security target or the guidance documentation of the product). The second goal of the method is to base as much as possible the evaluation work on real documentation used by the developer and not documentation written only for the Common Criteria. The evaluator will use the 'Collection of Evidence' method to limit as much as possible the developer documentation written after the development.

Important note: the method targets documentation problems that do not result in an evaluation that renders a 'FAIL' verdict. Typically, a 'documentation problem' could lead the evaluator to conclude that a security function requirement (SFR) has not been implemented and 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 must produce 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 to collect evidence for a specific evaluation

The developer and the evaluator must first assess the existing developer documentation for the evaluation tasks related to ADV[8], ALC[9], ATE[10]. Some initial documentation must be made available to the evaluator in relation to these evaluation activities. Otherwise, it is clear that some aspects of the evaluation will not be covered. The level of information provided should assure the evaluator and the CB that the evaluation outcome could be positive.

The assessment must take into account the targeted evaluation assurance level. Once this initial assessment is done, the evaluator decides if the scope to collect evidence is acceptable, and informs the CB of what type of documentation will be provided by the developer (corresponding to which evaluation activities or parts of), and what information will

[8] Development assurance class under Common Criteria
[9] Lifecycle support assurance class under Common Criteria
[10] Test assurance class under Common Criteria

be collected by the evaluator. The CB will then be able to approve or not the scope of the collection of evidence for the evaluation.

The evaluation verdict guarantees that the initial set of documents delivered is sufficient to carry out the evaluation. Indeed, it proves that the information which should have been provided by the developer (for strict conformance to the Common Criteria or for the evaluator's understanding) 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 help the evaluator to quickly understand the context of the product environment and the context of the evaluation. Therefore, the evaluator can take advantage of the training to determine if they will be able to collect evidence during the evaluation. It also helps to understand the target of evaluation (TOE) compared to the product.

The training will help the evaluator to:

- improve the ST evaluation relevance;
- gain a functional knowledge of the TOE before starting the FSP[11] and the guidance evaluation.

During the training, the developer must provide the evaluator

- a description of the ST by the ST writer;
- a 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 must provide these tools to the evaluator;
- access to design information to be able to understand the product's overall architecture (for TDS[12] evaluation activities).

If the evaluator concludes at the end of the initial training that the developer's input and the status of the documentation is unsuitable or insufficient for the 'collection of evidence', they would conclude that 'collection of evidence' is not feasible for the product under consideration. Therefore, the classical approach of the CEM would be preferred for the evaluation.

B2.1.4 The collection of evidence in practice

Some assurance components cannot be concerned by the collection of evidence.

- ASE[13]_xxx/APE[14]_xxx: the Security Target / Protection Profile is a document used for the whole evaluation, which will often be made public. This document must be complete and coherent as the evaluator will base their understanding of the evaluation on it.
- AGD[15]_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 further collection of evidence. However, 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 apply to the formal model itself.

Because the evaluator must not create but rather collect evidence, the information provided by the evaluator will mainly be in the form of a questionnaire constructed with open-ended questions that do not hint at the answer. Indeed, the questionnaire as a tool allows the information to be collected to focus on what is actually required by the evaluator,

[11] Functional specification assurance family of the Common Criteria.
[12] TOE design assurance family of the Common Criteria.
[13] Security target evaluation assurance class of the Common Criteria.
[14] Protection Profile evaluation assurance class of the Common Criteria.
[15] Guidance documents assurance class of the Common Criteria.

and to correspond to the information that is 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 must make a clear difference between the information collected (i.e. the answers given by the developer) and their own analysis/comments linked to these answers. Indeed, as the same document can include both developer answers and evaluator analysis, it is fundamental to make a clear distinction between them. For example, if the questionnaire is in 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 interview sessions occur and can decide to attend the sessions.

B2.1.5 Evaluator contributions endorsed by the developer

Once evidence has been collected, the evaluator sends it to the CB and to the developer. The developer must take the information collected as it become complementary evaluation evidence. This evidence must 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 to reuse, but this 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 makes a definite hypothesis and asks 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 purpose of the criteria is that developers should demonstrate familiarity with the TOE’s IT features, and that they have taken care with the security aspects, the developer must be able to answer to open questions corresponding to collection of evidence. The question corresponding to the 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 the 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 Minor deficiencies

The evaluator may address minor deficiencies in a developer-supplied deliverable by interviewing the developer and documenting their 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 minor deficiencies must 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 the creation of evidence is the importance of information to be confirmed by the developer in relation with the criteria. The minor deficiencies must 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 process. If however, correspondence has been inferred based on general similarities of the functions involved, then the work falls outside the scope of collection and correspond and moves to the category creation of evidence.

The design supplied by the developer may be found to be incomplete in certain respects. For example, it may not provide full details for all modules. There is scope for the evaluator to collect 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 must 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