EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUCC SCHEME

STATE-OF-THE-ART DOCUMENT

ACCREDITATION OF CBs FOR THE EUCC SCHEME

Version 1.6b, November 2024

DOCUMENT HISTORY

Date of change	Version	Modification	Clarification
19 February 2024	1.1	Document includes all comments of the Accreditation group under EUCC and was reviewed by ENISA for sharing with the EA and ECCG for further comments	Updates made for sharing
22 March 2024	1.2	Updated version based on ECCG and EA comments	Prepared for ECCG endorsement
30 April 2024	1.3	Improvement of the quality of the text Addition of a transition chapter	Updated version based on latest ECCG comments after the ECCG meeting of 15 April 2024
27 May 2024	1.5	Minor corrections in Chapter 8	Updated version prepared for EA comments
3 June 2024	1.6	Clarification of the accreditation scope (Chapter 7) Addition of an independence requirement (Chapter 8.2.1)	Updated version prepared for ECCG endorsement
19 June 2024	1.6a	Deletion of the standards reference dates	Endorsed for publication on 05/07/2024 by the ECCG
31 July 2024 – 15 November 2024	1.6b	Editorial changes Clarification of transition rules	Changes following the review by the European Commission and during 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 must 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

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 an overview of the requirements for the accreditation of Certification Bodies (CBs). As mentioned in the Annex to the EU Cybersecurity Act, the conformity assessments performed in the context of the EUCC must follow the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of conformity assessment bodies performing conformity assessment activities for the purpose of cybersecurity certification of ICT products.

This document specifically covers the accreditation of CBs as defined under Article 2 point 12 of the EUCC. 'Certification body' means a conformity assessment body as defined in Article 2, point (13), of Regulation (EC) No 765/2008, which performs certification activities.

Such certification activities cover:

- the review of the evaluation results and the verification of the evaluation technical report[2] in line with Article 9(1), points (d) and (e) of the EUCC;
- the issuance, renewal and withdrawal of EUCC certificates in line with Articles 9 to 14 and 16 to 20 of EUCC;
- monitoring activities, as defined in Article 26(1) of the EUCC;
- conformity and compliance activities, as defined in Articles 28 to 31 of the EUCC;
- vulnerability management and disclosure activities, as defined in Articles 35 and 36 of the EUCC.

The standard selected for the accreditation of CBs under the EUCC is EN ISO/IEC 17065:2012 in line with point 19 of the Annex to Regulation (EU) 2019/881. Among the requirements defined for CBs in that standard, many are related to the methodology to be applied by the CB during a conformity assessment.

These methodological elements are broad, and this state-of-the-art document provides the necessary interpretations to the necessary competences to perform conformity assessment activities for the purpose of cybersecurity certification of ICT products according to the Common Criteria together with the Common Evaluation Methodology.

Next to the requirements provided by the standard EN ISO/IEC 17065:2012, the Annex to Regulation (EU) 2019/881 sets out the main requirements for accreditation of conformity assessment bodies in general. Under paragraph 8.1 of this document, a mapping of these annexed requirements and the applicable standard of EN ISO/IEC 17065:2012 is provided.

The formal accreditation statement provided by the National Accreditation Body (NAB) to the CB sets forth that the CB complies with the conformity assessment requirements and that it is technically competent to carry out their related tasks.

This document must be used by NABs to accredit the CBs for EUCC, with the active support of the National Cybersecurity Certification Authority (NCCA)[3] in their monitoring and supervising role established in the respective Member State.

This document takes into consideration that Information Technology Security Evaluation Facilities (ITSEFs) are accredited for the EUCC scheme according to scheme requirements and related state-of-the-art documents, in particular to the state-of-the-art document related to the Accreditation of ITSEFs for the EUCC scheme, available on the ENISA website dedicated to certification[4].

[2] As defined under Article 2 point 6 of EUCC: 'evaluation technical report' means a document produced by an ITSEF to present the findings, verdicts and justifications obtained during the evaluation of an ICT product or a protection profile in line with the rules and obligations set out in this Regulation. ('ITSEF' means an Information Technology Security Evaluation Facility, which is a conformity assessment body as defined in Article 2, point (13), of Regulation (EC) No 765/2008 that performs evaluation tasks.).

[3] NCCAs mentioned in this document are acting on their monitoring and supervising role.

[4] https://certification.enisa.europa.eu/index_en

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 the body that is responsible to perform the accreditation for a conformity assessment body (CB and the ITSEF both need to be accredited for their conformity assessment activities) (Article 60(1) CSA).

Where the CB intends to certify for the assurance level high, the NCCA and the NAB should pay attention to the fact that the CB may want to avoid duplication of effort and to use the work undertaken during the accreditation process as much as possible in the authorisation process. Therefore, the accreditation body should 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 must 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:

- report the results of the accreditation assessment to the NCCA, including assessment reports and decisions on granting, extending, reducing, suspending, or withdrawing of accreditations for EUCC;
- apply an assessment programme to assess that the accredited conformity assessment bodies meet the requirements of accreditation;
- take appropriate measures to reduce the scope, suspend or withdrawn the accreditation of conformity assessment bodies where they are not compliant with the accreditation requirements, including those from the CSA.

In the case of possible infringements of the CSA, particularly related to the requirements in Annex of the CSA, the collaboration with the NCCA is important since 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 taken by the NAB, the NCCA must notify the European Commission in accordance with Article 61 CSA and relevant implementing regulation[5].

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 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 cannot obstruct the handling of complaints performed by the CB in line with EN ISO/IEC 17065:2012 concerning any:

- (potential) non-compliance of the CB related to the accreditation requirements annexes in Regulation (EU) 2019/881 (Cybersecurity Act- Article 58(7), point (c) and Article 58(7), points (h) and (i) CSA);
- (potential) non-compliance of the CB that is a public body (Article 58(7), point (d) CSA);
- complaints received related to the authorisation of a CB that may have an impact on the accreditation of the CB (for assurance level 'high' Article 58(7), point (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 and ITSEFs) activities and the monitoring and supervision of the CB that issues certificates of protection profiles, in line with Article 17(4) of Commission Implementing Regulation (EU) 2024/482 in an annual summary report and send this to the ECCG and ENISA[6].

[5] 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

[6] See Article 58(7), point (g) CSA.

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.

Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

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.

3 ACRONYMS AND DEFINITIONS

3.1 ACRONYMS

CB	Certification body
CC	Common Criteria for Information Technology Security Evaluation.
CEM	Common Methodology for Information Technology Security Evaluation
CSA	Cybersecurity Act
ENISA	European Union Agency for Cybersecurity
ETR	Evaluation technical report
EUCC	European Common Criteria-based cybersecurity certification scheme
ICT	Information and communications technology
ITSEF	Information Technology Security Evaluation Facility
NAB	National accreditation body

NCCA	National cybersecurity certification authority in its monitoring and supervising role
SOG-IS	Senior Officials Group – Information Systems Security
TA	Technical assessor
TE	Technical expert
TOE	Target of evaluation

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.

Certifier
'Certifier' means CB personnel performing technical activities such as review or decision taking.

Evaluator
'Evaluator' means ITSEF personnel performing evaluation activities.

4 SCOPE AND OBJECTIVE

CBs, including their staff, must be technically competent, impartial and perform their duties in a consistent manner when certifying a TOE under the EUCC.

EN ISO/IEC 17065:2012 applies to a very general and wide range of certification activities. This document is intended to be used for the accreditation of CBs for the EUCC. It includes interpretations of EN ISO/IEC 17065:2012 applicable to the cybersecurity certification of ICT products, and further EUCC requirements for CBs whose conformity is to be assessed during their accreditation.

5 APPLICABILITY OF INTERNATIONAL STANDARDS TO THE ACCREDITATION OF CBS

The Cybersecurity Act 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 standard must apply to the accreditation of CBs:

- EN ISO/IEC 17065:2012 - Conformity assessment – Requirements for bodies certifying products, processes and services' is binding for CB accreditation.

Note: 'ISO/IEC 19896 - IT security techniques - Requirements for the competence of IT security conformance assessment body personnel is currently being revised to define specific requirements for certifiers that should later be referred to in this document, as set out in Chapter 8.2 'Specific accreditation requirements'.

6 SCOPE OF THE ACCREDITATION OF A CB

The scope of accreditation must at least specify:

- The certification field:
  - ICT Cybersecurity Evaluation
- The certification 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 CB has proven technical competence to review the assessments and reports established by the ITSEFs in line with ISO/IEC 18045:2022, for example:
  - IT security certification up to EAL 3 augmented with ALC_FLR.2
- The reference to the scheme:
  - EUCC.

Technology and evaluation types from Annex in which the CB has proven technical competence must be referred to in the accreditation assessment report.

7 ACCREDITATION REQUIREMENTS

The CB accreditation requirements are as follows:

- those that need to be met by conformity assessment bodies as set out in the Annex to the CSA. These are provided in Section 8.1 'General accreditation requirements from the CSA';
- those applicable to CBs as indicated in the EUCC, in particular monitoring activities by the certification body (Article 26);
- those for bodies certifying products defined in ISO/IEC 17065:2012;
- those mentioned in Section 8.2 'Specific accreditation requirements' of this document.

7.1 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 the table below).

For information purposes, links to related requirements in EN ISO/IEC 17065:2012 that may support compliance of the CSA requirements are set out in the second column of the table below.

Requirements from the CSA Annex 'REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES'		Supporting EN ISO/IEC 17065:2012 requirement
1.	A conformity assessment body shall be established under national law and shall have legal personality.	EN ISO/IEC 17065:2012, 4.1.1
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 17065:2012, 4.2
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 17065:2012, 4.2
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 17065:2012, 4.2
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	EN ISO/IEC 17065:2012, 4.2

Requirements from the CSA Annex 'REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES'		Supporting EN ISO/IEC 17065:2012 requirement
	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.	
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.	EN ISO/IEC 17065:2012, 4.2
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 17065:2012, 4.2.3; 4.2.6; 4.2.7; 4.2.8 and 6.2.2
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 17065:2012, 4.2.2; 4.2.3; 4.2.5; 4.2.12; 6.1.1.2; 6.1.2 and 6.1.3
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 17065:2012, 6.1.1.1; 6.1.1.2 and 6.2.1
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 17065:2012, 6.1.1.1; 6.1.1.2; 6.2.1; 4.4; 4.6a); 5.1.2; 7.1.1; 7.1.2; 7.1.3; 7.3; 7.4.4; 7.10.1 7.10.2
(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.	

Requirements from the CSA Annex 'REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES'	Supporting EN ISO/IEC 17065:2012 requirement
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 17065:2012, 4.3.2; 6.2 and 7.3.1
12. The persons responsible for carrying out conformity assessment activities shall have the following: (d) sound technical and vocational training covering all conformity assessment activities; (e) satisfactory knowledge of the requirements of the conformity assessments they carry out and adequate authority to carry out those assessments; (f) appropriate knowledge and understanding of the applicable requirements and testing standards; (g) the ability to draw up certificates, records and reports demonstrating that conformity assessments have been carried out.	EN ISO/IEC 17065:2012, 6.1.1.2; 6.1.2 and 6.2.1
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 17065:2012, 4.2.3; 4.2.4 and 5.2
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.	
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.	EN ISO/IEC 17065:2012, 4.3
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 17065:2012, 4.5 and 6.1.1.3
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.	EN ISO/IEC 17065:2012, 7.2
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.	EN ISO/IEC 17065:2012, 4.4; 7.1 and 7.4.4
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	EN ISO/IEC 17065:2012

Requirements from the CSA Annex 'REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES'		Supporting EN ISO/IEC 17065:2012 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.	EN ISO/IEC 17025:2017 EN ISO/IEC 17065:2012, 6.2.1 and 6.2.2.1

7.2 SPECIFIC ACCREDITATION REQUIREMENTS

The requirements set out in CSA Annex and EN ISO/IEC 17065:2012 regarding independence, personnel, resources and selecting an ITSEF as specified below, must apply to the accreditation of a CB.

7.2.1 Independence

The independence criteria set out in CSA Annex point 2 must apply to the ICT product, ICT process, ICT service under evaluation.

The CB 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.

7.2.2 Certification body personnel

[EN ISO/IEC 17065:2012], 6.1 Certification body personnel

[EN ISO/IEC 17065:2012], 6.1.2 Management of competence for personnel involved in the certification process

The CB must establish, implement and maintain a procedure to manage the competencies of certifiers.

- The elements of competence, competency levels, knowledge, skills, experience and education must comply with the specific requirements for certifiers brought by the revision of ISO/IEC 19896:2018[7], once available.
- The knowledge required for certifying specific technologies and exercising different evaluation technique types are to be specified by the CB using the classification provided in the Annex on Technology and evaluation technique types.

The CB may use other classification criteria, as long as it can be mapped to the one provided in the Annex on Technology and evaluation technique types. Such mapping, and the supporting rationale, must be made available to the NABs and NCCA.

7.2.3 Resources for the evaluation

[EN ISO/IEC 17065:2012], 6.2 Resources for the evaluation

EN ISO/IEC 17065:2012 allows for two options as regards resources for evaluation:

1. The use of the CB internal resources, either directly employed by the CB or under its direct control;

2. The use of external resources, which might belong to different legal entities or may be other parts of the same legal entities.

[7] Users of this document may consider applying immediately the requirements established in the latest versions of the working drafts associated with this revision.

ISO/IEC 18045:2022 states in §9.2.2 and §9.2.3 that the evaluator and the certifier roles must be met by different entities. Moreover, ISO/IEC TS 23532-1:2021 that applies to ITSEF performing CC evaluations, states that: 'To maintain impartiality, the laboratory shall maintain proper separation between evaluators and other personnel inside the laboratory or outside the laboratory, but inside the parent organisation.'

Therefore, in the EUCC context, the use of internal resources of the CB to perform ITSEF activities must not be allowed.

In addition, where the CB and the ITSEF belong to the same legal entity:

- top-level management must not be involved in certification decision;
- top-level management must commit to preserve impartiality and prevent undue influence between certification and evaluation;
- the CB and ITSEF must have disjoint perimeters and operate independently in terms of:
  - working procedures;
  - competence management;
  - resource allocation.

  This implies some structural and organisational separation. Personnel that are involved in the evaluation activities must not be CB´s personnel and they must not be involved in the review and certification decision-making process. However, quality management may be shared between both accredited bodies.

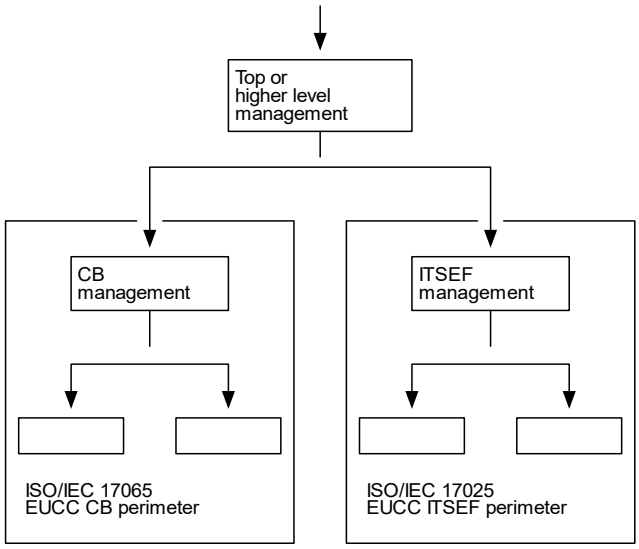

Figure 1: Structural separation between the CB and ITSEF parts of one legal entity

The CB must take responsibility for all the evaluation tasks outsourced to selected and approved ITSEFs. The outsourced activities, as well as the CB's responsibility for those outsourced tasks, must be reflected in the legally binding contract or agreement the CB enters into with its clients.

7.2.4 Requirements for CBs to select and approve ITSEFs

In response to EN ISO/IEC 17065:2012 §6.2.2.3, the CB must have a legally binding contract or agreement in place with each ITSEF it's working with. The agreements must include specific provisions on:

- The respective roles and responsibilities of both the CB and ITSEF for CC evaluation and certification tasks, in line with ISO/IEC 18045:2022 §9.2;

- The management of confidentiality, in particular for sensitive and/or proprietary information shared by the sponsor/developer as part of certification evidence, and evaluation results;
- Identification and prevention of conflict of interest, in line with EN ISO/IEC 17065:2012 6.1.3 item c).

Note: ITSEF must perform evaluation activities as specified in the CEM work units and provide verdicts on to the conformance of the evaluated product with the specified security requirements; the CB must review - and possibly discuss - the verdicts proposed by ITSEF, and based on a final ETR, confirm those verdicts and make a certification decision that must, when applicable, lead to the issuance of a EUCC certificate and certification report.

The CB must maintain a list of selected and approved ITSEFs for the outsourcing of evaluation tasks as part of EUCC certification projects.

The CB must have a process in place to assess that:

- selected and approved ITSEFs are appropriately accredited according to EN ISO/IEC 17025:2017 and applicable state-of-the-art documents, for the scope of evaluation activities that are relevant for the activities of the CB;
- the selected and approved ITSEFs continue to comply with rules and requirements covered by the contract or agreement they have with the CB.

The process must be documented in the CB's operating procedures, and records of assessment and monitoring of the selected and approved ITSEFs must be produced and securely stored for at least 5 years after the legally binding contract or agreement with an ITSEF has ceased to produce effect.

The CB must have a process in place to implement corrective actions for any breaches of the contract or agreement with an ITSEF of which it becomes aware.

7.3 TRANSITION

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

However, the issuance of certificates upon successful performance of all certification activities requires that the CB is accredited and where necessary authorized, 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 CB may not ultimately be accredited and, if necessary, authorised.

ANNEX TECHNOLOGY AND EVALUATION TECHNIQUE TYPES

This Annex provides a taxonomy of technology and evaluation technique types, with examples. This taxonomy should be used both to manage the competence of the CBs and for its assessment by 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.2 EVALUATION TECHNIQUE TYPES

The CB is expected to indicate the reference to the definition of applied methods used to support the certification activities under assessment for accreditation.

Some references are included in the following tables, where alternative methods can be applied if proved equivalent/acceptable by the CBs if they ensure that certification results meet the standard required by the scheme and the applicable state-of-the-art documents.

A.2.1 Source code review

Languages	Manual / automatic review	Reference to applied methods and/or tools (EUCC harmonised or CB 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 CB 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 15408:2022
Cryptographic protocols	Security assessment	[ISO/IEC 29128:2011] Verification of cryptographic protocols

A.2.3 Vulnerability analysis and penetration tests (generic)

Technologies embedded in the evaluated product	Known[8] attack technique	Reference to applied methods and/or tools (EUCC harmonised or CB internal)
Fill-in using codes from Technology types. Example: S1, S2, N1	Bypass	[ISO/IEC 20004:2015] Refining software vulnerability analysis under ISO/IEC 15408:2022 and ISO/IEC 18045:2022 [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	
	Race conditions	

[8] Unlike ITSEFs, the CBs do not need to have the capability of conducting special attacks using specialised/bespoke equipment. However, they still need to have a deep understanding of those attack techniques to review the evaluation reports.

Technologies embedded in the evaluated product	Known[8] attack technique	Reference to applied methods and/or tools (EUCC harmonised or CB internal)
	Tampering	
	Web application security	

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

Technologies embedded in the evaluated product	Known attack technique	Reference to applied methods and/or tools (EUCC harmonised or CB 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	Known attack technique	Reference to applied methods and/or tools (EUCC harmonised or CB 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)	

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