EUROPEAN UNION AGENCY
FOR CYBERSECURITY


# EUCC SCHEME

## DRAFT STATE-OF-THE-ART DOCUMENT

### ACCREDITATION OF CBs FOR THE EUCC SCHEME

Version 1.6a, June 2024

# DOCUMENT HISTORY

| Date of change | Version | Modification | Clarification |
|---|---|---|---|
| February 19th | 1.137M | 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 |
| 22/03/2024 | 1.2 | Updated version based on ECCG and EA comments | Prepared for ECCG endorsement |
| 30/04/2024 | 1.3 | Improvement of the quality of the text<br>Addition of a transition chapter | Updated version based on latest ECCG comments after the ECCG meeting of April 15 |
| 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)<br>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 and approved for publication on 16/07/2024 by the ECCG |

# LEGAL INFORMATION

## LEGAL NOTICE

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

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

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

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

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

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

## COPYRIGHT NOTICE



## CONTACT

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

## CONTENTS

# 1 INTRODUCTION

This draft state-of-the-art document as defined under Article 2 point 14 of Regulation (EU) 2024/482 is a legal supporting document under Implementing Regulation (EU) 2024/482 on establishing the Common Criteria-based cybersecurity certification scheme (EUCC) which provides the overview of requirements related to the accreditation of Certification Bodies (CBs). As mentioned in the EU Cybersecurity Act, the conformity assessments performed in the context of the EUCC shall follow the requirements of the relevant standard that is harmonized 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 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 in particular:

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

The standard selected for the accreditation of CBs under EUCC is ISO/IEC 17065. 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 generic, and this document provides the necessary interpretations and defines more specific requirements related to the necessary competences to perform conformity assessment activities for the purpose of cybersecurity certification of ICT products according to the Common Criteria in conjunction with the Common Evaluation Methodology.

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

The formal accreditation statement provided by the National Accreditation Body (NAB) to the CB implies that the CB is compliant with the indicated requirements for conformity assessment and that it is technically competent for their related tasks.

This document shall be used by NABs for the accreditation of CBs for EUCC, with the active support of the National Cybersecurity Certification Authority (NCCA[2]) in their monitoring and supervising role established in the respective Member State.

This document takes into consideration that 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 https://certification.enisa.europa.eu/index_en.

[1] 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 accordance 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.)

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

## 1.1 RESPONSIBILITIES OF THE NATIONAL ACCREDITATION BODY

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

Where the 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 authorization process. Therefore, the accreditation body should, wherever practical, use technical assessors (TAs) and technical experts (TEs) who can also be accepted by the NCCA and should consult with the NCCA if they are interested in including a suitable technical expert to participate in the accreditation process. TAs and TEs used by the NAB shall however operate under the sole responsibility of the NAB for their accreditation activities.

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

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

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

## 1.2 RESPONSIBILITIES OF THE NATIONAL CYBERSECURITY CERTIFICATION AUTHORITY

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

The monitoring and supervising national cybersecurity certification authorities (NCCAs) have the responsibility to actively assist and support the NAB in their monitoring and supervising tasks and need to share information and report to the NAB. This shall occur without prejudice to the handling of complaints performed by the CB in accordance with ISO/IEC 17065 with regards to:

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

The NCCA needs to include the active assistance and support provided to the NAB with regards to in the monitoring and supervision of the activities of CABs (CBs & ITSEFs) and the monitoring and supervision of the CB that issues certificates of protection profiles, in accordance with Article 17 (4) Commission Implementing Regulation (EU) 2024/482 in an annual summary report and send this to the European cybersecurity certification group (ECCG) and the EU Agency for Cybersecurity (ENISA)[3].

[3] See Article 58 (7) (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-CSA).

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 - Information technology — Security techniques — Evaluation criteria for IT security.

ISO/IEC 18045 - Information technology — Security techniques — Methodology for IT security evaluation.

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

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

## 3 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 |

## 4 DEFINITIONS

The definitions of the CSA and the EUCC apply to this document. In addition, the following definitions also apply to this document:

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

**Evaluator**
ITSEF personnel performing evaluation activities.

# 5 SCOPE AND OBJECTIVE

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

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

# 6 APPLICATION OF INTERNATIONAL STANDARDS TO THE ACCREDITATION OF CBS.

The Cybersecurity Act prescribes the obligation that schemes refer to international, European or national standards that are to be applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme.

In this respect the following standard shall apply to the accreditation of CBs:

- "ISO/IEC 17065 - 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 as to define specific requirements for certifiers, that should later be referred to in this state-of-the-art document, as detailed in chapter 8.2 "Specific accreditation requirements".

# 7 SCOPE OF THE ACCREDITATION OF A CB

The scope of accreditation shall 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 from ISO/IEC 15408 in which the CB has proven technical competence to review the assessments and reports established by the ITSEFs in accordance with ISO/IEC 18045, for example:
  - IT security certification up to EAL3 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 shall be detailed in the accreditation assessment report.

# 8 ACCREDITATION REQUIREMENTS

The CB accreditation requirements are the following:

- Those requirements that are to be met by conformity assessment bodies indicated in the Annex of the CSA. These are provided in section 8.1 "General accreditation requirements from the CSA";
- Those requirements applicable to CBs indicated in EUCC, in particular those related to Monitoring activities by the certification body (Article 26);
- The requirements for bodies certifying products defined in ISO/IEC 17065;
- Further requirements specified by this document, provided in section 8.2 "Specific accreditation requirements".

## 8.1 GENERAL ACCREDITATION REQUIREMENTS FROM THE CSA

Conformity assessment bodies that wish to be accredited shall meet the requirements indicated in the Annex of the CSA, included in the following table.

For information purposes, links to related requirements from ISO/IEC 17065 that may support compliance of the indicated CSA requirements are provided in the second column of the table.

| Requirement from CSA Annex "REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES" | | Supporting ISO/IEC 17065 requirement |
|---|---|---|
| 1. | A conformity assessment body shall be established under national law and shall have legal personality. | ISO/IEC 17065, 4.1.1 |
| 2. | A conformity assessment body shall be a third-party body that is independent of the organization or the ICT products, ICT services or ICT processes that it assesses. | ISO/IEC 17065, 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. | ISO/IEC 17065, 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 authorized representative of any of those parties. That prohibition shall not preclude the use of the ICT products assessed that are necessary for the operations of the conformity assessment body or the use of such ICT products for personal purposes. | ISO/IEC 17065, 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 maintenance of the ICT products, ICT services or ICT processes which are assessed, or represent parties engaged in those activities. The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to their conformity assessment activities. That prohibition shall apply, in particular, to consultancy services. | ISO/IEC 17065, 4.2 |
| 6. | If a conformity assessment body is owned or operated by a public entity or institution, the independence and absence of any conflict | ISO/IEC 17065, 4.2 |

| Requirement from CSA Annex "REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES" | | Supporting ISO/IEC 17065 requirement |
|---|---|---|
| | of interest shall be ensured between the national cybersecurity certification authority and the conformity assessment body, and shall be documented. | |
| 7. | Conformity assessment bodies shall ensure that the activities of their subsidiaries and subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities. | ISO/IEC 17065, 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. | ISO/IEC 17065, 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. | ISO/IEC 17065, 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: | ISO/IEC 17065, 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. | |
| 11. | A conformity assessment body shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner, and shall have access to all necessary equipment and facilities. | ISO/IEC 17065, 4.3.2; 6.2 and 7.3.1 |
| 12. | The persons responsible for carrying out conformity assessment activities shall have the following: | ISO/IEC 17065, 6.1.1.2; 6.1.2 and 6.2.1 |
| (d) | sound technical and vocational training covering all conformity assessment activities; | |

| Requirement from CSA Annex "REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES" | Supporting ISO/IEC 17065 requirement |
|---|---|
| (e) satisfactory knowledge of the requirements of the conformity assessments they carry out and adequate authority to carry out those assessments;<br>(f) appropriate knowledge and understanding of the applicable requirements and testing standards;<br>(g) the ability to draw up certificates, records and reports demonstrating that conformity assessments have been carried out. | |
| 13. The impartiality of the conformity assessment bodies, of their top-level management, of the persons responsible for carrying out conformity assessment activities, and of any subcontractors shall be guaranteed. | ISO/IEC 17065, 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. | ISO/IEC 17065, 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. | ISO/IEC 17065, 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. | ISO/IEC 17065, 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. | ISO/IEC 17065, 4.4; 7.1 and 7.4.4 |
| 19. Conformity assessment bodies shall meet the requirements of the relevant standard that is harmonized under Regulation (EC) No 765/2008 for the accreditation of conformity assessment bodies performing certification of ICT products, ICT services or ICT processes. | ISO/IEC 17065 |
| 20. Conformity assessment bodies shall ensure that testing laboratories used for conformity assessment purposes meet the requirements of the relevant standard that is harmonized under Regulation (EC) No 765/2008 for the accreditation of laboratories performing testing. | ISO/IEC 17025<br>ISO/IEC 17065, 6.2.1 and 6.2.2.1 |

## 8.2 SPECIFIC ACCREDITATION REQUIREMENTS

In addition to the requirements included in ISO/IEC 17065, the following requirements shall apply to the accreditation of a CB.

### 8.2.1 Independence

The independence criteria from CSA Annex point 2 shall apply to the ICT product, ICT process, ICT service under evaluation.

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

### 8.2.2 Certification body personnel

[ISO/IEC 17065], 6.1 Certification body personnel

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

The CB shall establish, implement and maintain a procedure for management of competencies of certifiers where:

- The elements of competence, competency levels, knowledge, skills, experience and education shall comply with the specific requirements for certifiers brought by the revision of ISO/IEC 19896[4], 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 Annex, Technology and evaluation technique types.

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

### 8.2.3 Resources for evaluation

[ISO/IEC 17065], 6.2 Resources for evaluation

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

- The use of the CB internal resources, either directly employed by the CB or under its direct control;
- The use of external resources, which might belong to different legal entities or may be other parts of the same legal entities.

ISO/IEC 18045 states in §9.2.2 and §9.2.3 that the evaluator and the certifier roles shall be fulfilled by different entities. Moreover, ISO/IEC TS 23532 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 organization.”

Therefore, in the EUCC context, only the use of external resources shall be possible as illustrated in the following figures. ITSEFs, whether they belong to the same organization or are part of a different organization than the CB, shall be seen as subcontractors/outsourced resources in the sense of ISO/IEC 17065.

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

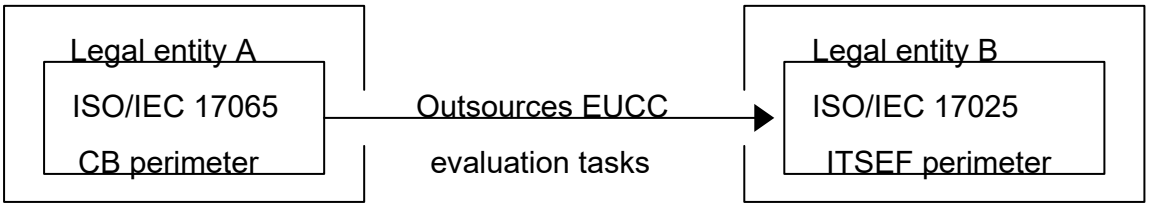


*Figure 1: Outsourcing to an ITSEF part of a different organization*

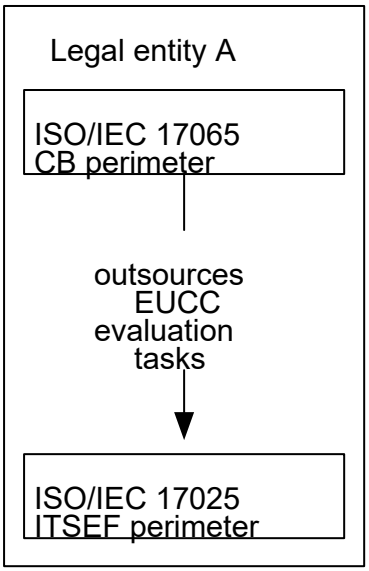


*Figure 2: Outsourcing to an ITSEF part of the same legal entity*

In the second option, illustrated in Figure 2, some additional requirements are to be fulfilled by the legal entity to which the CB and the ITSEF belong:

- Top-level management shall not be involved in certification decision,
- Top-level management shall commit to preserve impartiality and prevent undue influence between certification and evaluation,
- When another part of the same legal entity acts as ITSEF, CB and ITSEF shall have disjoint perimeters and operate independently in terms of:
  - Working procedures,
  - Competence management,
  - Resource allocation.

  This implies some structural and organizational separation. Personnel involved in evaluation activities shall not be CB´s personnel and shall not be involved in the review and certification decision-making process. However, without prejudice to the previous requirements, Quality Management may be mutualized between both accredited bodies.

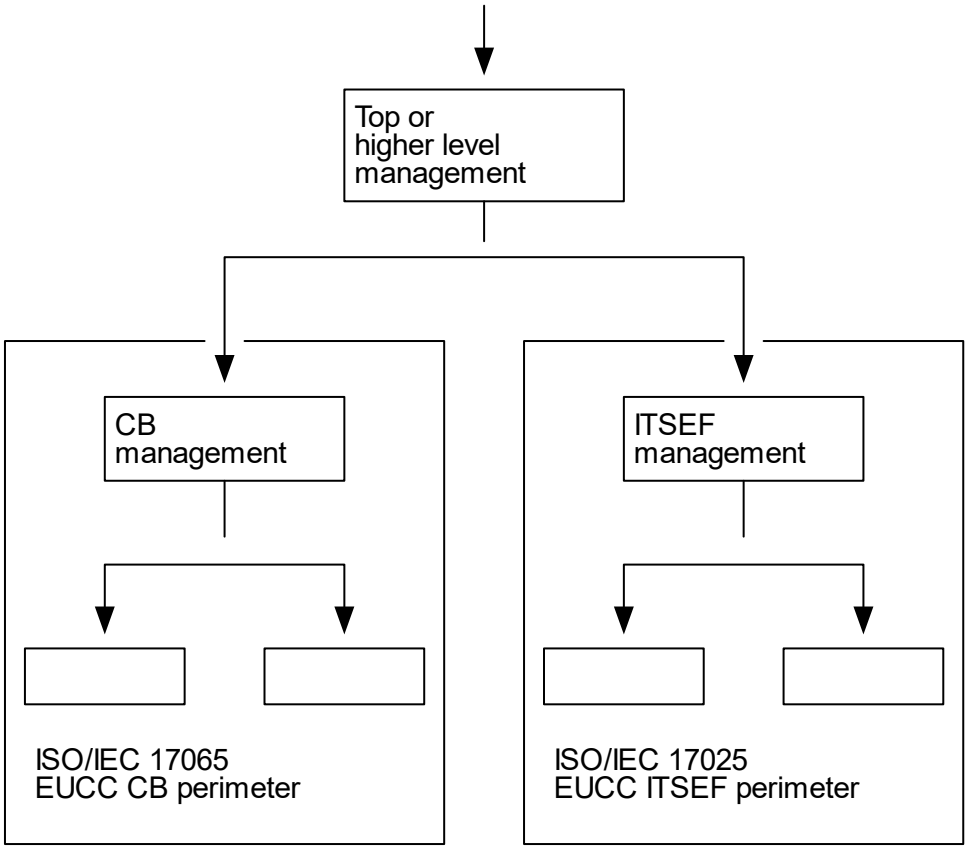


*Figure 3: Structural separation between CB and ITSEF parts of one legal entity*

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

### 8.2.4 Requirements for CBs for the selection and approval of ITSEFs

In response to ISO/IEC 17065 §6.2.2.3, the CB shall have a legally binding contract or agreement in place with each ITSEF it's working with, that includes specific provisions for:

- The respective roles and responsibilities of both the CB and the ITSEF regarding CC evaluation and certification tasks, in line with ISO/IEC 18045 §9.2;
- The management of confidentiality, in particular as regards 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 ISO/IEC 17065 6.1.3 item c).

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

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

The CB shall have a process in place to assess:

- That selected and approved ITSEFs are appropriately accredited according to ISO/IEC 17025 and according to the state-of-the-art document “ACCREDITATION OF ITSEFs FOR THE EUCC SCHEME”, for the scope of evaluation activities that are relevant for the activities of the CB;
- That, at any time, the selected and approved ITSEFs continue to comply with rules and requirements covered by the contract or agreement they have with the CB.

Such process shall be documented in the CB’s operating procedures, and records of assessment and monitoring of the selected and approved ITSEFs shall be produced and securely stored for a period of at least five (5) years after the legally binding contract or agreement with an ITSEF has ceased to produce effect.

The CB shall 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.

## 8.3 TRANSITION

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

The issuance of certificates following successful performance of all certification activities shall only be possible once the CB has been accredited and where necessary authorized.

# 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 for the management of the competence of the CBs and for its assessment by NABs.

## TECHNOLOGY TYPES

### Hardware and software architectures, OS and applicative security

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

### 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 | |

### 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 |

## 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, provided that they ensure that certification results meet the standard required by the scheme and the applicable state-of-the-art documents.

### Source code review

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

### Cryptographic analysis

| Object | Principle of the method | Reference to applied methods and/or tools (EUCC harmonized 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 |
| Cryptographic protocols | Security assessment | [ISO/IEC 29128:2011] Verification of cryptographic protocols |

### Vulnerability analysis and penetration tests (generic)

| Technologies embedded in the evaluated product | Known[5] attack technique | Reference to applied methods and/or tools (EUCC harmonized 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 and ISO/IEC 18045<br>[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 | |

[5] Unlike ITSEFs, the CBs do not need to have the capability of conducting special attacks using specialized/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[5] attack technique | Reference to applied methods and/or tools (EUCC harmonized or CB internal) |
|---|---|---|
| | Race conditions | |
| | Tampering | |
| | Web application security | |

### 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 harmonized 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 | |

### 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 harmonized 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