

Commission 18 December 2024	Implementing Regulation	(EU) 2024/3144	of	L 3144	1	19.12.2024
--------------------------------	----------------------------	----------------	----	--------	---	------------

**▼B****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)**

**(Text with EEA relevance)**

**CHAPTER I****GENERAL PROVISIONS***Article 1***Subject matter and scope**

This Regulation sets out the European Common Criteria-based cybersecurity certification scheme (EUCC).

This Regulation applies to all information and communication technologies ('ICT') products, including their documentation, which are submitted for certification under the EUCC, and to all protection profiles which are submitted for certification as part of the ICT process leading to the certification of ICT products.

*Article 2***Definitions**

For the purposes of this Regulation, the following definitions shall apply:

**▼M1**

- (1) 'Common Criteria' means the Common Criteria for Information Technology Security Evaluation, as set out in standards ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022 or ISO/IEC 15408-5:2022, or set out in Common Criteria for Information Technology Security Evaluation, version CC:2022, Parts 1 through 5, published by the participants of the Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security;
- (2) 'Common Evaluation Methodology' means the Common Methodology for Information Technology Security Evaluation, as set out in standard ISO/IEC 18045:2022, or the Common Methodology for Information Technology Security Evaluation, version CEM:2022, published by the participants of the Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security;

**▼B**

- (3) 'target of evaluation' means an ICT product or part thereof, or a protection profile as part of an ICT process, which is subjected to cybersecurity evaluation to receive EUCC certification;
- (4) 'security target' means a claim of implementation-dependent security requirements for a specific ICT product;

**▼B**

- (5) ‘protection profile’ means an ICT process that lays down the security requirements for a specific category of ICT products, addressing implementation-independent security needs, and that may be used to assess ICT products falling into that specific category for the purpose of their certification;
- (6) ‘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;
- (7) ‘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;
- (8) ‘AVA\_VAN level’ means an assurance vulnerability analysis level that indicates the degree of cybersecurity evaluation activities carried out to determine the level of resistance against potential exploitability of flaws or weaknesses in the target of evaluation in its operational environment as set out in the Common Criteria;
- (9) ‘EUCC certificate’ means a cybersecurity certificate issued under the EUCC for ICT products, or for protection profiles that can be used exclusively in the ICT process of certification of ICT products;
- (10) ‘composite product’ means an ICT product that is evaluated together with another underlying ICT product that has already received an EUCC certificate and on whose security functionality the composite ICT product depends;
- (11) ‘national cybersecurity certification authority’ means an authority designated by a Member State pursuant to Article 58(1) of Regulation (EU) 2019/881;
- (12) ‘certification body’ means a conformity assessment body as defined in Article 2, point (13), of Regulation (EC) No 765/2008, which performs certification activities;
- (13) ‘technical domain’ means a common technical framework related to a particular technology for the harmonised certification with a set of characteristic security requirements;
- (14) ‘state-of-the-art document’ means a document which specifies evaluation methods, techniques and tools that apply to the certification of ICT products, or security requirements of a generic ICT product category, or any other requirements necessary for certification, in order to harmonise evaluation, in particular of technical domains or protection profiles;
- (15) ‘market surveillance authority’ means an authority defined in Article 3(4) of Regulation (EU) 2019/1020.

▼ **M1***Article 3***Evaluation standards**

1. The following standards shall apply to evaluations performed under the EUCC scheme:

(a) the Common Criteria;

(b) the Common Evaluation Methodology.

2. Until 31 December 2027, a certificate may be issued under the EUCC scheme applying either of the following standards:

(a) ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 or ISO/IEC 15408-3:2008;

(b) Common Criteria for Information Technology Security Evaluation, version 3.1, revision 5, published by the participants of the Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security;

(c) ISO/IEC 18045:2008;

(d) Common Methodology for Information Technology Security Evaluation, revision 5, version 3.1, published by the participants of the Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security.

3. Until 31 December 2027, a certificate applying the standards referred to in paragraph 1 may be issued under the EUCC scheme claiming conformance to a protection profile that has applied the standards listed in paragraph 2.

4. A certificate applying the standards referred to in paragraph 1 may also be issued under the EUCC scheme claiming conformance to a protection profile that has applied either of the following standards, provided that the use of such protection profile is required under Commission Implementing Regulation (EU) 2016/799 <sup>(1)</sup>, Regulation (EU) No 910/2014 of the European Parliament and of the Council <sup>(2)</sup> or Commission Implementing Decision (EU) 2016/650 <sup>(3)</sup>:

<sup>(1)</sup> Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) No 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components (OJ L 139, 26.5.2016, p. 1, ELI: [http://data.europa.eu/eli/reg\\_impl/2016/799/oj](http://data.europa.eu/eli/reg_impl/2016/799/oj)).

<sup>(2)</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73, ELI: <http://data.europa.eu/eli/reg/2014/910/oj>).

<sup>(3)</sup> Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ L 109, 26.4.2016, p. 40, ELI: [http://data.europa.eu/eli/dec\\_impl/2016/650/oj](http://data.europa.eu/eli/dec_impl/2016/650/oj)).

**▼ M1**

- (a) Common Criteria for Information Technology Security Evaluation, version 3.1, revision 1 to 4, published by the participants of the Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security;
- (b) Common Methodology for Information Technology Security Evaluation, version 3.1., revision 1 to 4, published by the participants of the Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security.

**▼ B***Article 4***Assurance levels**

1. Certification bodies shall issue EUCC certificates at assurance level ‘substantial’ or ‘high’.
2. EUCC certificates at assurance level ‘substantial’ shall correspond to certificates that cover AVA\_VAN level 1 or 2.
3. EUCC certificates at assurance level ‘high’ shall correspond to certificates that cover AVA\_VAN level 3, 4 or 5.
4. The assurance level confirmed in a EUCC certificate shall distinguish between the conformant and augmented use of the assurance components as specified in the Common Criteria in accordance with Annex VIII.
5. Conformity assessment bodies shall apply those assurance components on which the selected AVA\_VAN level depends in accordance with the standards referred to in Article 3.

*Article 5***Methods for certifying ICT products**

1. Certification of an ICT product shall be carried out against its security target:
  - (a) as defined by the applicant; or

**▼ M1**

- (b) claiming conformance to a certified protection profile as part of the ICT process, where the ICT product falls in the ICT product category covered by that protection profile.

**▼ B**

2. Protection profiles shall be certified for the sole purpose of the certification of ICT products falling in the specific category of ICT products covered by the protection profile.

**▼B***Article 6***Conformity self-assessment**

A conformity self-assessment within the meaning of Article 53 of Regulation (EU) 2019/881 shall not be permitted.

## CHAPTER II

**CERTIFICATION OF ICT PRODUCTS***SECTION I**Specific standards and requirements for evaluation**Article 7***Evaluation criteria and methods for ICT products**

1. An ICT product submitted for certification shall, as a minimum, be evaluated in accordance with the following:

- (a) the applicable elements of the standards referred to in Article 3;
- (b) the security assurance requirements classes for vulnerability assessment and independent functional testing, as set out in the evaluation standards referred to in Article 3;
- (c) the level of risk associated with the intended use of the ICT products concerned pursuant to Article 52 of Regulation (EU) 2019/881 and their security functions that support the security objectives set out in Article 51 of Regulation (EU) 2019/881;
- (d) the applicable state-of-the-art documents listed in Annex I; and
- (e) the applicable certified protection profiles listed in Annex II.

2. In exceptional and duly justified cases, a conformity assessment body may request to refrain from applying the relevant state-of-the-art document. In such cases the conformity assessment body shall inform the national cybersecurity certification authority with a duly reasoned justification for its request. The national cybersecurity certification authority shall assess the justification for an exception and, where justified, approve it. Pending the decision of the national cybersecurity certification authority, the conformity assessment body shall not issue any certificate. The national cybersecurity certification authority shall notify the approved exception, without undue delay, to the European Cybersecurity Certification Group, which may issue an opinion. The national cybersecurity certification authority shall take utmost account of the opinion of the European Cybersecurity Certification Group.

**▼B**

3. Certification of ICT products at AVA\_VAN level 4 or 5 shall only be possible in the following scenarios:

- (a) where the ICT product is covered by any technical domain listed in Annex I, it shall be evaluated in accordance with the applicable state-of-the-art documents of those technical domains,
- (b) where the ICT product falls into a category of ICT products covered by a certified protection profile that includes AVA\_VAN levels 4 or 5 and that has been listed as a state-of-the-art protection profile in Annex II, it shall be evaluated in accordance with the evaluation methodology specified for that protection profile,
- (c) where points a) and b) of this paragraph are not applicable and where the inclusion of a technical domain in Annex I or of a certified protection profile in Annex II is unlikely in the foreseeable future, and only in exceptional and duly justified cases, subject to the conditions set out in paragraph 4.

4. Where a conformity assessment body considers to be in an exceptional and duly justified case referred to in point c) of paragraph 3, it shall notify the intended certification to the national cybersecurity certification authority with a justification and a proposed evaluation methodology. The national cybersecurity certification authority shall assess the justification for an exception and, where justified, approve or amend the evaluation methodology to be applied by the conformity assessment body. Pending the decision of the national cybersecurity certification authority, the conformity assessment body shall not issue any certificate. The national cybersecurity certification authority shall report, without undue delay, the intended certification to the European Cybersecurity Certification Group, which may issue an opinion. The national cybersecurity certification authority shall take utmost account of the opinion of the European Cybersecurity Certification Group.

5. In the case of an ICT product undergoing a composite product evaluation in accordance with the relevant state-of-the-art documents, the ITSEF that carried out the evaluation of the underlying ICT product shall share the relevant information with the ITSEF performing the evaluation of the composite ICT product.

*SECTION II**Issuance, renewal and withdrawal of EUCC certificates**Article 8***▼M1****Information necessary for certification and evaluation**

1. An applicant for certification under EUCC shall provide or otherwise make available to the certification body and the ITSEF all information necessary for the certification and evaluation activities.

**▼B**

2. The information referred to in paragraph 1 shall include all relevant evidence in accordance with the sections on ‘Developer action elements’ in the appropriate format as set out in the sections on ‘Content and presentation of evidence element’ of the Common Criteria and Common Evaluation Methodology for the selected assurance level and associated security assurance requirements. The evidence shall include, where necessary, details on the ICT product and its source code in accordance with this Regulation, subject to safeguards against unauthorised disclosure.

3. Applicants for certification may provide to the certification body and ITSEF appropriate evaluation results from prior certification pursuant to:

- (a) this Regulation;
- (b) another European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881;
- (c) a national scheme referred to in Article 49 of this Regulation.

4. Where the evaluation results are pertinent to its tasks, the ITSEF may reuse the evaluation results provided that such results conform to the applicable requirements and its authenticity is confirmed.

5. Where the certification body allows the product to undergo a composite product certification, the applicant for certification shall make available to the certification body and the ITSEF all necessary elements, where applicable, in accordance with the state-of-the-art document.

6. Applicants for certification shall also provide the certification body and the ITSEF with the following information:

- (a) the link to their website containing the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881;
- (b) a description of the applicant’s vulnerability management and vulnerability disclosure procedures.

7. All relevant documentation referred to in this Article shall be retained by the certification body, the ITSEF and the applicant for a period of 5 years after the expiry of the certificate.



**▼B***Article 9***Conditions for issuance of an EUCC certificate**

1. The certification bodies shall issue an EUCC certificate where all of the following conditions are met:

- (a) the category of ICT product falls within the scope of the accreditation, and where applicable of the authorisation, of the certification body and the ITSEF involved in the certification;
- (b) the applicant for certification has signed a statement undertaking all commitments listed in paragraph 2;
- (c) the ITSEF has concluded the evaluation without objection in accordance with the evaluation standards, criteria and methods referred to in Articles 3 and 7;
- (d) the certification body has concluded the review of the evaluation results without objection;
- (e) the certification body has verified that the evaluation technical reports provided by the ITSEF are consistent with the provided evidence and that the evaluation standards, criteria and methods referred to in Articles 3 and 7 have been correctly applied.

2. The applicant for certification shall undertake the following commitments:

- (a) to provide the certification body and the ITSEF with all the necessary complete and correct information, and to provide additional necessary information if requested;
- (b) not to promote the ICT product as being certified under the EUCC before the EUCC certificate has been issued;
- (c) to promote the ICT product as being certified only with respect to the scope set out in the EUCC certificate;
- (d) to cease immediately the promotion of the ICT product as being certified in the event of the suspension, withdrawal or expiry of the EUCC certificate;
- (e) to ensure that the ICT products sold with reference to the EUCC certificate are strictly identical to the ICT product subject to the certification;
- (f) to respect the rules of use of the mark and label established for the EUCC certificate in accordance with Article 11.

3. In the case of an ICT product undergoing a composite product certification, in accordance with the relevant state-of-the-art documents, the certification body that carried out the certification of the underlying ICT product shall share the relevant information with the certification body performing the certification of the composite ICT product.



#### *Article 10*

##### **Content and format of an EUCC certificate**

1. An EUCC certificate shall include at least the information set out in Annex VII.
2. The scope and boundaries of the certified ICT product shall be unambiguously specified in the EUCC certificate or the certification report, indicating whether the entire ICT product has been certified or only parts thereof.
3. The certification body shall provide the applicant with the EUCC certificate at least in electronic form.
4. The certification body shall produce a certification report in accordance with Annex V for each EUCC certificate it issues. The certification report shall be based on the evaluation technical report issued by the ITSEF. The evaluation technical report and the certification report shall indicate the specific evaluation criteria and methods referred to in Article 7 used for the evaluation.
5. The certification body shall provide the national cybersecurity certification authority and ENISA with every EUCC certificate and every certification report in electronic form.

#### *Article 11*

##### **Mark and label**

1. The holder of a certificate may affix a mark and label to a certified ICT product. Mark and label demonstrate that the ICT product has been certified in accordance with this Regulation. Mark and label shall be affixed in accordance with this Article and with Annex IX.
2. The mark and label shall be affixed visibly, legibly and indelibly to the certified ICT product or its data plate. Where that is not possible or not warranted on account of the nature of the product, it shall be affixed to the packaging and to the accompanying documents. Where the certified ICT product is delivered in the form of software, the mark and label shall visibly, legibly and indelibly appear in its accompanying documentation or this documentation shall be made easily and directly accessible to users by means of a website.
3. The mark and label shall be set out as in Annex IX and contain:
  - (a) the assurance level and the AVA\_VAN level of the certified ICT product;
  - (b) the unique identification of the certificate, consisting of:
    - (1) the name of the scheme;
    - (2) the name and the reference number of the accreditation of the certification body that has issued the certificate;
    - (3) year and month of issuance;
    - (4) identification number assigned by the certification body that has issued the certificate.

**▼B**

4. The mark and label shall be accompanied by a QR code with a link to a website containing at least:

- (a) the information on the validity of the certificate;
- (b) the necessary certification information as set out in Annexes V and VII;
- (c) the information to be made publicly available by the holder of the certificate in accordance with Article 55 of Regulation (EU) 2019/881; and
- (d) where applicable, the historic information related to the specific certification or certifications of the ICT product to enable traceability.

*Article 12***Period of validity of an EUCC certificate**

1. The certification body shall set a period of validity for each EUCC certificate issued taking into account the characteristics of the certified ICT product.

2. The period of validity of the EUCC certificate shall not exceed 5 years.

3. By derogation from paragraph 2 that period may exceed 5 years, subject to the prior approval of the national cybersecurity certification authority. The national cybersecurity certification authority shall notify the European Cybersecurity Certification Group of the granted approval without undue delay.

*Article 13***Review of an EUCC certificate**

1. Upon request of the holder of the certificate or for other justified reasons, the certification body may decide to review the EUCC certificate for an ICT product. The review shall be carried out in accordance with Annex IV. The certification body shall determine the extent of the review. Where necessary for the review, the certification body shall request the ITSEF to perform a re-evaluation of the certified ICT product.

2. Following the results of the review, and where applicable of the re-evaluation, the certification body shall:

- (a) confirm the EUCC certificate;
- (b) withdraw the EUCC certificate in accordance with Article 14;
- (c) withdraw the EUCC certificate in accordance with Article 14 and issue a new EUCC certificate with an identical scope and an extended validity period; or
- (d) withdraw the EUCC certificate in accordance with Article 14 and issue a new EUCC certificate with a different scope.

3. The certification body may decide to suspend, without undue delay, the EUCC certificate in accordance with Article 30, pending remedial action by the holder of the EUCC certificate.

*Article 14***Withdrawal of an EUCC certificate**

1. Without prejudice to Article 58(8), point (e), of Regulation (EU) 2019/881, an EUCC certificate shall be withdrawn by the certification body that issued that certificate.
2. The certification body referred to in paragraph 1 shall notify the national cybersecurity certification authority of the withdrawal of the certificate. It shall also notify ENISA of such withdrawal in view of facilitating the performance of its task under Article 50 of Regulation (EU) 2019/881. The national cybersecurity certification authority shall notify other relevant market surveillance authorities.
3. The holder of an EUCC certificate may request the withdrawal of the certificate.

## CHAPTER III

**CERTIFICATION OF PROTECTION PROFILES***SECTION I**Specific standards and requirements for evaluation**Article 15***Evaluation criteria and methods**

1. A protection profile shall be evaluated, as a minimum, in accordance with the following:
  - (a) the applicable elements of the standards referred to in Article 3;
  - (b) the level of risk associated with the intended use of the ICT products concerned pursuant to Article 52 of Regulation (EU) 2019/881 and their security functions that support the security objectives set out in Article 51 of that; and
  - (c) the applicable state-of-the-art documents listed in Annex I. A protection profile covered by a technical domain shall be certified against the requirements set out in that technical domain.
2. In exceptional and duly justified cases, a conformity assessment body may certify a protection profile without applying the relevant state-of-the-art documents. In such cases, it shall inform the competent national cybersecurity certification authority and provide a justification for the intended certification without application of the relevant state-of-the-art documents as well as the proposed evaluation methodology. The national cybersecurity certification authority shall assess the justification and, where justified, approve the non-application of the relevant state-of-the-art documents, and approve or amend, where appropriate, the evaluation methodology to be applied by the

**▼B**

conformity assessment body. Pending the decision of the national cybersecurity certification authority, the conformity assessment body shall not issue any certificate for the protection profile. The national cybersecurity certification authority shall notify, without undue delay, the authorised non-application of the relevant state-of-the-art documents to the European Cybersecurity Certification Group, which may issue an opinion. The national cybersecurity certification authority shall take utmost account of the opinion of the European Cybersecurity Certification Group.

*SECTION II**Issuing, renewing and withdrawing EUCC certificates for protection profiles***▼M1***Article 16***Information necessary for certification and evaluation of protection profiles**

An applicant for certification of a protection profile shall provide or otherwise make available to the certification body and the ITSEF all information necessary for the certification and evaluation activities in a complete and correct form. Article 8(2), (3), (4) and (7) shall apply *mutatis mutandis*.

**▼B***Article 17***Issuance of EUCC certificates for protection profiles****▼M1**


---

**▼B**

2. Articles 9 and 10 shall apply *mutatis mutandis*.
3. The ITSEF shall evaluate whether a protection profile is complete, consistent, technically sound and effective for the intended use and the security objectives of the ICT product's category covered by that protection profile.
4. A protection profile shall be certified solely by:
  - (a) a national cybersecurity certification authority or another public body accredited as certification body; or
  - (b) a certification body, upon prior approval by the national cybersecurity certification authority for each individual protection profile.

*Article 18***Period of validity of an EUCC certificate for protection profiles**

1. The certification body shall set a period of validity for each EUCC certificate.
2. The period of validity may be up to the lifetime of the protection profile concerned.

**▼B***Article 19***Review of an EUCC certificate for protection profiles**

1. Upon request of the holder of the certificate or for other justified reasons, the certification body may decide to review an EUCC certificate for a protection profile. The review shall be carried out by applying the conditions set out in Article 15. The certification body shall determine the extent of the review. Where necessary for the review, the certification body shall request the ITSEF to perform a re-evaluation of the certified protection profile.

2. Following the results of the review, and where applicable of the re-evaluation, the certification body shall do one of the following:

- (a) confirm the EUCC certificate;
- (b) withdraw the EUCC certificate in accordance with Article 20;
- (c) withdraw the EUCC certificate in accordance with Article 20 and issue a new EUCC certificate with an identical scope and an extended validity period;
- (d) withdraw the EUCC certificate in accordance with Article 20 and issue a new EUCC certificate with a different scope.

*Article 20***Withdrawal of an EUCC certificate for a protection profile**

1. Without prejudice to Article 58(8), point (e) of Regulation (EU) 2019/881, an EUCC certificate for a protection profile shall be withdrawn by the certification body that issued that certificate. Article 14 shall apply *mutatis mutandis*.

2. A certificate for a protection profile issued in accordance with Article 17(4), point (b) shall be withdrawn by the national cybersecurity certification authority that approved that certificate.

## CHAPTER IV

**CONFORMITY ASSESSMENT BODIES****▼M1***Article 20a***Specification of requirements for accreditation of conformity assessment bodies**

The accreditation of conformity assessment bodies shall take into account the specification of requirements for accreditation of certification bodies and ITSEFs as laid down in the applicable state-of-the-art documents listed in point 2 of Annex I.

*Article 21***Additional or specific requirements for a certification body**

1. A certification body shall be authorised by the national cybersecurity certification authority to issue EUCC certificates at assurance level ‘high’ where that body demonstrates that, in addition to meeting the requirements laid down in Article 60(1) and the Annex to Regulation (EU) 2019/881 regarding accreditation of conformity assessment bodies, the following:

- (a) it has the expertise and competences required for the certification decision at assurance level ‘high’;
- (b) it conducts its certification activities in cooperation with an ITSEF authorised in accordance with Article 22; and
- (c) it has the requisite competences and put in place appropriate technical and operational measures to effectively protect confidential and sensitive information for assurance level ‘high’, in addition to the requirements set out in Article 43.

2. The national cybersecurity certification authority shall assess whether a certification body fulfils all the requirements set out in paragraph 1. That assessment shall include at least structured interviews and a review of at least one pilot certification performed by the certification body in accordance with this Regulation.

In its assessment, the national cybersecurity certification authority may reuse any appropriate evidence from prior authorisation or similar activities granted pursuant to:

- (a) this Regulation;
- (b) another European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881;
- (c) a national scheme referred to in Article 49 of this Regulation.

3. The national cybersecurity certification authority shall produce an authorisation report which is subject to peer review in accordance with Article 59(3), point (d), of Regulation (EU) 2019/881.

4. The national cybersecurity certification authority shall specify the ICT product categories and protection profiles to which the authorisation extends. The authorisation shall be valid for a period no longer than the validity of the accreditation. It may be renewed upon request provided that the certification body still meets the requirements set out in this Article. For the renewal of the authorisation, no pilot evaluations are required.

5. The national cybersecurity certification authority shall withdraw the authorisation of the certification body where it no longer meets the conditions set out in this Article. Upon withdrawal of the authorisation, the certification body shall cease immediately promoting itself as an authorised certification body.

*Article 22***Additional or specific requirements for an ITSEF**

1. An ITSEF shall be authorised by the national cybersecurity certification authority to carry out the evaluation of ICT products which are subject to certification under the assurance level 'high', where the ITSEF demonstrates that, in addition to meeting the requirements laid down in Article 60(1) and the Annex to Regulation (EU) 2019/881 regarding accreditation of conformity assessment bodies, it complies with all of the following conditions:

- (a) it has the necessary expertise for performing the evaluation activities to determine the resistance to state-of-the-art cyberattacks carried out by actors with significant skills and resources;
- (b) for the technical domains and protection profiles, which are part of the ICT process for those ICT products, it has:
  - (1) the expertise to perform the specific evaluation activities necessary to methodically determine a target of evaluation's resistance against skilled attackers in its operational environment assuming an attack potential of 'moderate' or 'high' as set out in the standards referred to in Article 3;
  - (2) the technical competences as specified in the state-of-the-art documents listed in Annex I;
- (c) it has the requisite competences and put in place appropriate technical and operational measures to effectively protect confidential and sensitive information for assurance level 'high' in addition to the requirements set out in Article 43.

2. The national cybersecurity certification authority shall assess whether an ITSEF fulfils all the requirements set out in paragraph 1. That assessment shall include at least structured interviews and a review of at least one pilot evaluation performed by the ITSEF in accordance with this Regulation.

3. In its assessment, the national cybersecurity certification authority may reuse any appropriate evidence from prior authorisation or similar activities granted pursuant to:

- (a) this Regulation;
- (b) another European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881;
- (c) a national scheme referred to in Article 49 of this Regulation.

4. The national cybersecurity certification authority shall produce an authorisation report which is subject to peer review in accordance with Article 59(3), point (d) of Regulation (EU) 2019/881.



**▼B**

5. The national cybersecurity certification authority shall specify the ICT product categories and protection profiles to which the authorisation extends. The authorisation shall be valid for period no longer than the validity of the accreditation. It may be renewed upon request provided that the ITSEF still meets the requirements set out in this Article. For the renewal of the authorisation, no pilot evaluations should be required.

6. The national cybersecurity certification authority shall withdraw the authorisation of the ITSEF where it no longer meets the conditions set out in this Article. Upon withdrawal of the authorisation, the ITSEF shall stop promoting itself as being an authorised ITSEF.

**▼M1****▼B**

## CHAPTER V

**MONITORING, NON-CONFORMITY AND NON-COMPLIANCE***SECTION 1****Compliance monitoring****Article 25***Monitoring activities by the national cybersecurity certification authority**

1. Without prejudice to Article 58(7) of Regulation (EU) 2019/881, the national cybersecurity certification authority shall monitor the compliance of:

- (a) the certification body and the ITSEF with their obligations pursuant to this Regulation and Regulation (EU) 2019/881;
- (b) the holders of an EUCC certificate with their obligations pursuant to this Regulation and Regulation (EU) 2019/881;
- (c) the certified ICT products with the requirements set out in the EUCC;
- (d) the assurance expressed in the EUCC certificate addressing the evolving threat landscape.

2. The national cybersecurity certification authority shall perform its monitoring activities in particular on the basis of:

- (a) information coming from certification bodies, national accreditation bodies and relevant market surveillance authorities;
- (b) information resulting from its own or another authority's audits and investigations;
- (c) sampling, carried out in accordance with paragraph 3;
- (d) complaints received.

**▼B**

3. The national cybersecurity certification authority shall, in cooperation with other market surveillance authorities, sample annually at least 4% of the EUCC certificates as determined by a risk assessment. Upon request and acting on behalf of the competent national cybersecurity certification authority, certification bodies and, if necessary, ITSEF shall assist that authority in monitoring compliance.

4. The national cybersecurity certification authority shall select the sample of certified ICT products to be checked using objective criteria, including:

- (a) product category;
- (b) assurance levels of products;
- (c) holder of a certificate;
- (d) certification body and, where applicable, the subcontracted ITSEF;
- (e) any other information brought to the authority's attention.

5. The national cybersecurity certification authority shall inform the holders of the EUCC certificate about the selected ICT products and the selection criteria.

6. The certification body that certified the sampled ICT product shall, upon request of the national cybersecurity certification authority, with the assistance of the respective ITSEF, conduct additional review in accordance with the procedure laid down in Section IV.2 of Annex IV and inform the national cybersecurity certification authority of the results.

7. Where the national cybersecurity certification authority has sufficient reason to believe that a certified ICT product is no longer in compliance with this Regulation or Regulation (EU) 2019/881, it may carry out investigations or make use of any other monitoring powers set out in Article 58(8) of Regulation (EU) 2019/881.

8. The national cybersecurity certification authority shall inform the certification body and ITSEF concerned about ongoing investigations regarding selected ICT products.

9. Where the national cybersecurity certification authority identifies that an ongoing investigation concerns ICT products that are certified by certification bodies established in other Member States, it shall inform thereof the national cybersecurity certification authorities of the relevant Member States in order to collaborate in the investigations, where relevant. Such national cybersecurity certification authority shall also notify the European Cybersecurity Certification Group of the cross-border investigations and the subsequent results.

**▼B***Article 26***Monitoring activities by the certification body**

1. The certification body shall monitor:
  - (a) the compliance of the holders of a certificate with their obligations under this Regulation and Regulation (EU) 2019/881 towards the EUCC certificate that was issued by the certification body;
  - (b) the compliance of the ICT products it has certified with their respective security requirements;
  - (c) the assurance expressed in the certified protection profiles.
2. The certification body shall undertake its monitoring activities on the basis of:
  - (a) the information provided on the basis of the commitments of the applicant for certification referred to in Article 9(2);
  - (b) information resulting from activities of other relevant market surveillance authorities;
  - (c) complaints received;
  - (d) vulnerability information that could impact the ICT products it has certified.
3. The national cybersecurity certification authority may draw up rules for a periodical dialogue between certification bodies and holders of EUCC certificates to verify and report on compliance with the commitments made pursuant to Article 9(2), without prejudice to activities related to other relevant market surveillance authorities.

*Article 27***Monitoring activities by the holder of the certificate**

1. The holder of an EUCC certificate shall perform the following tasks to monitor the conformity of the certified ICT product with its security requirements:
  - (a) monitor vulnerability information regarding the certified ICT product, including known dependencies by its own means but also in consideration of:
    - (1) a publication or a submission regarding vulnerability information by a user or security researcher referred to in Article 55(1), point (c) of Regulation (EU) 2019/881;
    - (2) a submission by any other source;
  - (b) monitor the assurance expressed in the EUCC certificate.

**▼B**

2. The holder of an EUCC certificate shall work in cooperation with the certification body, the ITSEF, and, where applicable, the national cybersecurity certification authority to support their monitoring activities.

*SECTION II****Conformity and compliance****Article 28***Consequences of non-conformity of a certified ICT product or protection profile**

1. Where a certified ICT product or protection profile does not conform with the requirements laid down in this Regulation and in Regulation (EU) 2019/881, the certification body shall inform the holder of the EUCC certificate about the identified non-conformity and request remedial actions.

2. Where an instance of non-conformity with the provisions of this Regulation might affect compliance with other relevant Union legislation, which provides for the possibility to demonstrate the presumption of conformity with the requirements of that legal act by using the EUCC certificate, the certification body shall inform the national cybersecurity certification authority without delay. The national cybersecurity certification authority shall immediately notify the market surveillance authority responsible for such other relevant Union legislation regulation about the instance of non-conformity identified.

3. Upon receipt of the information referred to in paragraph 1, the holder of the EUCC certificate shall within the time period set by the certification body, which shall not exceed 30 days, propose to the certification body the remedial action necessary to address the non-conformity.

4. The certification body may suspend, without undue delay, the EUCC certificate in accordance with Article 30 in case of emergency, or where the holder of the EUCC certificate does not duly cooperate with the certification body.

5. The certification body shall carry out a review in accordance with Articles 13 and 19, assessing whether the remedial action addresses the non-conformity.

6. Where the holder of the EUCC certificate does not propose appropriate remedial action during the period referred to in paragraph 3, the certificate shall be suspended in accordance with Article 30 or withdrawn in accordance with Articles 14 or 20.

7. This Article shall not apply to cases of vulnerabilities affecting a certified ICT product, which shall be handled in accordance with Chapter VI.

*Article 29***Consequences of non-compliance by the holder of the certificate**

1. Where the certification body finds that:

- (a) the holder of the EUCC certificate or the applicant for certification is not compliant with its commitments and obligations as set out in Articles 9(2), 17(2), 27 and 41; or

**▼B**

- (b) the holder of the EUCC certificate does not comply with Article 56 (8) of Regulation (EU) 2019/881 or Chapter VI of this Regulation;

it shall set a time period of not more than 30 days within which the holder of the EUCC certificate shall take remedial action.

**▼M1**

2. Where the holder of the EUCC certificate does not propose appropriate remedial action during the time period referred to in paragraph 1, the certificate shall be suspended in accordance with Article 30 or withdrawn in accordance with Article 14 or Article 20.

**▼B**

3. Continued or recurring infringement by the holder of the EUCC certificate of the obligations referred to in paragraph 1 shall trigger the withdrawal of the EUCC certificate in accordance with Articles 14 or Article 20.

4. The certification body shall inform the national cybersecurity certification authority of the findings referred to in paragraph 1. Where the instance of non-compliance affects compliance with other relevant Union legislation, the national cybersecurity certification authority shall immediately notify the market surveillance authority responsible for such other relevant Union legislation about the instance of non-compliance identified.

*Article 30***Suspension of the EUCC certificate**

1. Where this Regulation refers to suspension of an EUCC certificate, the certification body shall suspend an EUCC certificate concerned for a period appropriate to the circumstances triggering suspension, that does not exceed 42 days. The suspension period shall begin on the day following the day of the decision of the certification body. The suspension shall not affect the validity of the certificate.

2. The certification body shall notify the holder of the certificate and the national cybersecurity certification authority of the suspension without undue delay and shall provide the reasons for the suspension, the requested actions to be taken and the suspension period.

3. Certification holders shall notify the purchasers of the ICT products concerned about the suspension and the reasons provided by the certification body for the suspension, except those parts of the reasons the sharing of which would constitute a security risk or which contain sensitive information. This information shall also be made publicly available by the holder of the certificate.

4. Where other relevant Union legislation provides for a presumption of conformity based on certificates issued under the provisions of this Regulation, the national cybersecurity certification authority shall inform the market surveillance authority responsible for such other relevant Union legislation about the suspension.

5. The suspension of a certificate shall be notified to ENISA in accordance with Article 42(3).

6. In duly justified cases, the national cybersecurity certification authority may authorise an extension of the period of suspension of an EUCC certificate. The total period of suspension may not exceed 1 year.

**▼B***Article 31***Consequences of non-compliance by the conformity assessment body**

1. In case of non-compliance by a certification body with its obligations, or by the relevant certification body in case of identifying non-compliance by an ITSEF, the national cybersecurity certification authority shall, without undue delay:

- (a) identify, with the support of the concerned ITSEF, the potentially affected EUCC certificates;
- (b) where necessary, request evaluation activities to be performed on one or more ICT products or protection profiles by either the ITSEF which performed the evaluation, or any other accredited and, where applicable, authorised ITSEF that may be in a better technical position to support that identification;
- (c) analyse the impacts of non-compliance;
- (d) notify the holder of the EUCC certificate affected by non-compliance.

2. On the basis of the measures referred to in paragraph 1, the certification body shall adopt either of the following decisions with respect to each affected EUCC certificate:

- (a) maintain the EUCC certificate unaltered;
- (b) withdraw the EUCC certificate in accordance with Article 14 or Article 20, and, where appropriate, issue a new EUCC certificate.

3. On the basis of the measures referred to in paragraph 1, the national cybersecurity certification authority shall:

- (a) where necessary, report the non-compliance of the certification body or related ITSEF to the national accreditation body;
- (b) where applicable, assess the potential impact on the authorisation.

## CHAPTER VI

**VULNERABILITY MANAGEMENT AND DISCLOSURE***Article 32***Scope of vulnerability management**

This Chapter applies to ICT products for which an EUCC certificate was issued.

*SECTION 1****Vulnerability management****Article 33***Vulnerability management procedures**

1. The holder of an EUCC certificate shall establish and maintain all necessary vulnerability management procedures in accordance with the rules laid down in this Section and, where necessary, supplemented by the procedures set out in EN ISO/IEC 30111.

**▼B**

2. The holder of an EUCC certificate shall maintain and publish appropriate methods for receiving information on vulnerabilities related to their products from external sources, including users, certification bodies and security researchers.
3. Where a holder of an EUCC certificate detects or receives information about a potential vulnerability affecting a certified ICT product, it shall record it and carry out a vulnerability impact analysis.
4. When a potential vulnerability impacts a composite product, the holder of the EUCC certificate shall inform the holder of dependent EUCC certificates about potential vulnerability.
5. In response to a reasonable request by the certification body that issued the certificate, the holder of an EUCC certificate shall transmit all relevant information about potential vulnerabilities to that certification body.

*Article 34***Vulnerability impact analysis**

1. Vulnerability impact analysis shall refer to the target of evaluation and the assurance statements contained in the certificate. Vulnerability impact analysis shall be carried out in a timeframe appropriate for the exploitability and criticality of the potential vulnerability of the certified ICT product.
2. Where applicable, an attack potential calculation shall be performed in accordance with the relevant methodology included in the standards referred to in Article 3 and the relevant state-of-the-art documents listed in Annex I, in order to determine the exploitability of the vulnerability. The AVA\_VAN level of the EUCC certificate shall be taken into account.

*Article 35***Vulnerability impact analysis report**

1. The holder shall produce a vulnerability impact analysis report where the impact analysis shows that the vulnerability has a likely impact on the conformity of the ICT product with its certificate.
2. The vulnerability impact analysis report shall contain an assessment of the following elements:
  - (a) the impact of the vulnerability on the certified ICT product;
  - (b) possible risks associated with the proximity or availability of an attack;
  - (c) whether the vulnerability may be remedied;
  - (d) where the vulnerability may be remedied, possible resolutions of the vulnerability.
3. The vulnerability impact analysis report shall, where applicable, contain details about the possible means of exploitation of the vulnerability. Information pertaining to possible means of exploitation of the vulnerability shall be handled in accordance with appropriate security measures to protect its confidentiality and ensure, where necessary, its limited distribution.

**▼B**

4. The holder of an EUCC certificate shall transmit a vulnerability impact analysis report to the certification body or the national cybersecurity certification authority in accordance with Article 56(8) of Regulation (EU) 2019/881, without undue delay.

5. Where the vulnerability impact analysis report determines that the vulnerability is not residual within the meaning of standards referred to in Article 3, and that it can be remedied, Article 36 shall apply.

6. Where the vulnerability impact analysis report determines that the vulnerability is not residual and that it cannot be remedied, the EUCC certificate shall be withdrawn in accordance with Article 14.

7. The holder of the EUCC certificate shall monitor any residual vulnerabilities to ensure that it cannot be exploited in case of the changes in the operational environment.

*Article 36***Vulnerability remediation**

The holder of an EUCC certificate shall submit a proposal for an appropriate remedial action to the certification body. Certification body shall review the certificate in accordance with Article 13. The scope of the review shall be determined by the proposed remediation of the vulnerability.

*SECTION II****Vulnerability disclosure****Article 37***Information shared with the national cybersecurity certification authority**

1. The information provided by the certification body to the national cybersecurity certification authority shall include all elements necessary for the national cybersecurity certification authority to understand the impact of the vulnerability, the changes to be made to the ICT product and, where available, any information from the certification body on the broader implications of the vulnerability for other certified ICT products.

2. The information provided in accordance with paragraph 1 shall not contain details of the means of exploitation of the vulnerability. This provision is without prejudice to the investigative powers of the national cybersecurity certification authority.

*Article 38***Cooperation with other national cybersecurity certification authorities**

1. The national cybersecurity certification authority shall share the relevant information received in accordance with Article 37 with other national cybersecurity certification authorities and ENISA.



**▼B**

2. Other national cybersecurity certification authorities may decide to further analyse the vulnerability or, after informing the holder of the EUCC certificate, request the relevant certification bodies to assess whether the vulnerability may affect other certified ICT products.

*Article 39***Publication of the vulnerability**

Upon withdrawal of a certificate, the holder of the EUCC certificate shall disclose and register any publicly known and remediated vulnerability in the ICT product on the European vulnerability database, established in accordance with Article 12 of Directive (EU) 2022/2555 of the European Parliament and of the Council <sup>(1)</sup> or other online repositories referred to in Article 55(1), point (d) of Regulation (EU) 2019/881.

## CHAPTER VII

**RETENTION, DISCLOSURE AND PROTECTION OF INFORMATION***Article 40***Retention of records by certification bodies and the ITSEF**

1. The ITSEF and certification bodies shall maintain a record system, which shall contain all documents produced in connection with each evaluation and certification they perform.

2. Certification bodies and the ITSEF shall store the records in a secure manner and shall keep those records for the period necessary for the purposes of this Regulation and for at least 5 years after the withdrawal of the relevant EUCC certificate. When the certification body has issued a new EUCC certificate in accordance with Article 13(2), point (c), it shall retain the documentation of the withdrawn EUCC certificate together with and as long as for the new EUCC certificate.

*Article 41***Information made available by the holder of a certificate**

1. The information referred to in Article 55 of Regulation (EU) 2019/881 shall be available in a language that can be easily accessible to users.

2. The holder of an EUCC certificate shall store the following securely for the period necessary for the purposes of this Regulation and for at least 5 years after the withdrawal of the relevant EUCC certificate:

- (a) records of the information provided to the certification body and to the ITSEF during the certification process;
- (b) specimen of the certified ICT product.

---

<sup>(1)</sup> Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

**▼B**

3. When the certification body has issued a new EUCC certificate in accordance with Article 13(2), point (c), the holder shall retain the documentation of the withdrawn EUCC certificate together with and as long as for the new EUCC certificate.

4. Upon request by the certification body or the national cybersecurity certification authority, the holder of an EUCC certificate shall make available the records and copies referred to in paragraph 2.

*Article 42***Information to be made available by ENISA**

1. ENISA shall publish the following information on the website referred to in Article 50(1) of Regulation (EU) 2019/881:

- (a) all EUCC certificates;
- (b) the information on the status of an EUCC certificate, notably whether it is in force, suspended, withdrawn, or expired;
- (c) certification reports corresponding to each EUCC certificate;
- (d) a list of accredited conformity assessment bodies;
- (e) a list of authorised conformity assessment bodies;
- (f) the state-of-the-art documents listed in Annex I
- (g) the opinions of the European Cybersecurity Certification Group referred to in Article 62(4), point (c), of Regulation (EU) 2019/881;
- (h) peer assessment reports issued in accordance with Article 47.

2. The information referred to in paragraph 1 shall be made available at least in English.

3. Certification bodies and, where applicable, national cybersecurity certification authorities shall inform ENISA without delay about their decisions which affect the content or the status of an EUCC certificate referred to in paragraph 1, point (b).

4. ENISA shall ensure that the information published in accordance with paragraph 1 points (a), (b) and (c), clearly identifies the versions of a certified ICT product which are covered by an EUCC certificate.

*Article 43***Protection of information**

Conformity assessment bodies, national cybersecurity certification authorities, ECCG, ENISA, the Commission and all other parties shall ensure the security and protection of business secrets and other confidential information, including trade secrets, as well as the preserving intellectual property rights, and take the necessary and appropriate technical and organisational measures.



## CHAPTER VIII

## MUTUAL RECOGNITION AGREEMENTS WITH THIRD COUNTRIES

*Article 44***Conditions**

1. Third countries willing to certify their products in accordance with this Regulation, and who wish to have such certification recognised within the Union, shall conclude a mutual recognition agreement with the Union.

2. The mutual recognition agreement shall cover the applicable assurance levels for certified ICT products and, where applicable, protection profiles.

3. Mutual recognition agreements referred to in paragraph 1, may only be concluded with third countries that meet the following conditions:

(a) have an authority that:

- (1) is a public body, independent of the entities it supervises and monitors in terms of organisational and legal structure, financial funding and decision making;
- (2) has appropriate monitoring and supervising powers to carry out investigations and is empowered to take appropriate corrective measures to ensure compliance;
- (3) has an effective, proportionate and dissuasive penalty system to ensure compliance;
- (4) agrees to collaborate with the European Cybersecurity Certification Group and ENISA to exchange best practice and relevant developments in the field of cybersecurity certification and to work towards a uniform interpretation of the currently applicable evaluation criteria and methods, amongst others, by applying harmonised documentation that is equivalent to the state-of-the-art documents listed in Annex I

(b) have an independent accreditation body performing accreditations using equivalent standards to those referred to in Regulation (EC) No 765/2008;

(c) commit that the evaluation and certification processes and procedures will be carried out in a duly professional manner, taking into account compliance with the international standards referred to in this Regulation, in particular in Article 3;

(d) have the capacity to report previously undetected vulnerabilities and an established, adequate vulnerability management and disclosure procedure in place;

(e) have established procedures that enable it to effectively lodge and handle complaints and provide effective legal remedy for the complainant;

**▼B**

- (f) establishing a mechanism for cooperation with other Union and Member States' bodies relevant to the cybersecurity certification under this Regulation including the sharing of information about the possible non-compliance of certificates, monitoring relevant developments in the field of certification and ensuring a joint approach on certification maintenance and review.

4. In addition to the conditions set out in paragraph 3, a mutual recognition agreement referred to in paragraph 1 covering assurance level 'high' may only be concluded with third countries where also the following conditions are met:

- (a) the third country has an independent and public cybersecurity certification authority performing or delegating evaluation activities necessary to allow certification under assurance level 'high' that are equivalent to the requirements and procedures laid down for national cybersecurity authorities in this Regulation and in Regulation (EU) 2019/881;
- (b) the mutual recognition agreement establishes a joint mechanism equivalent to the peer assessment for EUCC certification to enhance the exchange of practices and jointly solve issues in the area of evaluation and certification.

## CHAPTER IX

## PEER ASSESSMENT OF CERTIFICATION BODIES

*Article 45***Peer assessment procedure**

1. A certification body issuing EUCC certificates at assurance level 'high' shall undergo a peer assessment on a regular basis and at least every 5 years. The different types of peer assessment are listed in Annex VI.

2. The European Cybersecurity Certification Group shall draw up and maintain a schedule of peer assessments ensuring that such periodicity is respected. Except in duly justified cases, peer assessments shall be performed on-site.

3. The peer assessment may rely on evidence gathered in the course of previous peer assessments or equivalent procedures of the peer-assessed certification body or national cybersecurity certification authority, provided that:

- (a) the results are not older than 5 years;
- (b) the results are accompanied by a description of the peer assessment procedures established for that scheme where they relate to a peer assessment conducted under a different certification scheme;
- (c) the peer assessment report referred to in Article 47 specifies which results were reused with or without further assessment.

**▼B**

4. Where a peer assessment covers a technical domain, the concerned ITSEF shall also be assessed.
5. The peer-assessed certification body and, where necessary, the national cybersecurity certification authority shall ensure that all relevant information is made available to the peer assessment team.
6. The peer assessment shall be carried out by a peer assessment team set up in accordance with Annex VI.

*Article 46***Peer assessment phases**

1. During the preparatory phase, the members of the peer assessment team shall review the certification body's documentation, covering its policies and procedures, including the use of state-of-the-art documents.
2. During site visit phase, the peer assessment team assesses the body's technical competence and, where applicable, the competence of an ITSEF that performed at least one ICT product evaluation covered by peer assessment.
3. The duration of the site visit phase may be extended or reduced depending on such factors as the possibility of reusing existing peer assessment evidence and results or the number of ITSEF and technical domains for which the certification body issues certificates.
4. If applicable, the peer assessment team shall determine the technical competence of each ITSEF by visiting its technical laboratory or laboratories and interviewing its evaluators as regards the technical domain and related specific attack methods.
5. In the reporting phase, the assessment team shall document their findings in a peer assessment report including a verdict and, where applicable, a list of observed non-conformities, each graded by a criticality level.
6. The peer assessment report must be first discussed with the peer-assessed certification body. Following those discussions, the peer-assessed certification body establishes a schedule of the measures to be taken to address the findings.

*Article 47***Peer assessment report**

1. The peer assessment team shall provide the peer-assessed certification body with a draft of the peer assessment report.
2. The peer-assessed certification body shall submit to the peer assessment team comments regarding the findings and a list of commitments to address the shortcomings identified in the draft peer assessment report.

**▼B**

3. The peer assessment team shall submit to the European Cybersecurity Certification Group a final peer assessment report, which shall also include the comments and the commitments made by the peer-assessed certification body. The peer assessment team shall also include their position on the comments and on whether those commitments are sufficient to address the shortcomings identified.

4. Where non-conformities are identified in the peer-assessment report, the European Cybersecurity Certification Group may set an appropriate time limit for the peer-assessed certification body to address the non-conformities.

5. The European Cybersecurity Certification Group shall adopt an opinion on the peer assessment report:

- (a) where the peer-assessment report does not identify non-conformities or where non-conformities have been appropriately addressed by the peer-assessed certification body, the European Cybersecurity Certification Group may issue a positive opinion and all relevant documents shall be published on ENISA's certification website;
- (b) where the peer-assessed certification body does not address the non-conformities appropriately within the set time limit, the European Cybersecurity Certification Group may issue a negative opinion that shall be published on ENISA's certification website, including the peer assessment report and all relevant documents.

6. Prior to the publication of the opinion, all sensitive, personal or proprietary information shall be removed from the published documents.

## CHAPTER X

## MAINTENANCE OF THE SCHEME

*Article 48***Maintenance of the EUCC**

1. The Commission may request the European Cybersecurity Certification Group to adopt an opinion in view of maintaining the EUCC and to undertake the necessary preparatory works.

2. The European Cybersecurity Certification Group may adopt an opinion to endorse state-of-the-art documents.

3. State-of-the-art documents which have been endorsed by the European Cybersecurity Certification Group shall be published by ENISA.

**▼M1**

4. Unless specified otherwise in Annex I or II, state-of-the-art documents shall apply from the date of application of the amending act by which they have been incorporated in Annex I or II.

▼ B

CHAPTER XI  
FINAL PROVISIONS

*Article 49*

**National schemes covered by the EUCC**

1. In accordance with Article 57(1) of Regulation (EU) 2019/881 and without prejudice to Article 57(3) of that Regulation, all national cybersecurity certification schemes and the related procedures for ICT products and ICT processes that are covered by the EUCC shall cease to produce effects from 12 months after the entry into force of this Regulation.
2. By derogation from Article 50, a certification process may be initiated under a national cybersecurity certification scheme within 12 months from the entry into force of this Regulation provided that the certification process is finalised not later than 24 months after entry into force of this Regulation.
3. Certificates issued under national cybersecurity certification schemes may be subject to review. New certificates replacing the reviewed certificates shall be issued in accordance with this Regulation.

▼ M1

4. When conducting the review referred to in paragraph 3 within two years of the issuance of initial certificate and where such a review leads to the issuance of a new certificate in accordance with this Regulation, the standards listed in Article 3(2) may be applied. The date of issuance of the initial certificate shall be understood as the date of issuance of the last certificate for a ICT product or protection profile on which the current certification is based on.

▼ B

*Article 50*

**Entry into force**

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

It shall apply from 27 February 2025.

Chapter IV and Annex V shall apply from the date of entry into force of this Regulation.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

**▼ M1***ANNEX I***State-of-the-art documents supporting technical domains and other state-of-the-art documents**

1. State-of-the-art documents supporting technical domains at AVA\_VAN level 4 or 5:
  - (a) the following documents related to the harmonised evaluation of technical domain ‘smart cards and similar devices’:
    - (1) ‘Minimum ITSEF requirements for security evaluations of smart cards and similar devices’, version 1.1;
    - (2) ‘Minimum Site Security Requirements’, version 1.1;
    - (3) ‘Application of Common Criteria to integrated circuits’, version 1.1;
    - (4) ‘Security Architecture requirements (ADV\_ARC) for smart cards and similar devices’, version 1.1;
    - (5) ‘Certification of ‘open’ smart card products’, version 1.1;
    - (6) ‘Composite product evaluation for smart cards and similar devices’, version 1.1;
    - (7) ‘Application of Attack Potential to Smartcards and Similar Devices’, version 1.2;
  - (b) the following documents related to the harmonised evaluation of technical domain ‘hardware devices with security boxes’:
    - (1) ‘Minimum ITSEF requirements for security evaluations of hardware devices with security boxes’, version 1.1;
    - (2) ‘Minimum Site Security Requirements’, version 1.1;
    - (3) ‘Application of Attack Potential to hardware devices with security boxes’, version 1.2.
2. State-of-the-art documents related to the harmonised accreditation of conformity assessment bodies:
  - (a) ‘Accreditation of ITSEFs for the EUCC’, version 1.1 for accreditations issued before 8 July 2025.
  - (b) ‘Accreditation of ITSEFs for the EUCC’, version 1.6c, for accreditations that are newly issued or reviewed after 8 July 2025.
  - (c) ‘Accreditation of CBs for the EUCC’, version 1.6b.



*ANNEX II***Protection profiles certified at AVA\_VAN level 4 or 5**

1. For the category of remote qualified signature and seal creation devices:
  - (1) EN 419241-2:2019 – Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing ;
  - (2) EN 419221-5:2018 - Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services
2. Protection profiles that have been adopted as state-of-the-art documents:

[BLANK]

**▼B***ANNEX III***Recommended protection profiles (illustrating technical domains from Annex I)**

Protection profiles used in certification of ICT products falling under the below stated ICT product category:

(a) for the category of machine readable travel documents:

- (1) PP Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011-MA-01;
- (2) PP for a Machine Readable Travel Document with "ICAO Application" Extended Access Control, BSI-CC-PP-0056-2009;
- (3) PP for a Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE, BSI-CC-PP-0056-V2-2012-MA-02;
- (4) PP for a Machine Readable Travel Document with "ICAO Application" Basic Access Control, BSI-CC-PP-0055-2009;

(b) for the category of secure signature creation devices:

- (1) EN 419211-1:2014 - Protection profiles for secure signature creation device - Part 1: Overview
- (2) EN 419211-2:2013 - Protection profiles for secure signature creation device - Part 2: Device with key generation;
- (3) EN 419211-3:2013 - Protection profiles for secure signature creation device - Part 3: Device with key import;
- (4) EN 419211-4:2013 - Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application
- (5) EN 419211-5:2013 - Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application;
- (6) EN 419211-6:2014 - Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application;

(c) for the category of digital tachographs:

- (1) Digital Tachograph - Tachograph Card, as referred in Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 (Annex 1C);
- (2) Digital Tachograph - Vehicle unit as referred in Annex IB of Commission Regulation (EC) No. 1360/2002 intended to be installed in road transport vehicles;

**▼B**

- (3) Digital Tachograph - External GNSS Facility (EGF PP) as referred in Annex 1C of Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 of the European Parliament and of the Council;
  - (4) Digital Tachograph - Motion Sensor (MS PP) as referred in Annex 1C of Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 of the European Parliament and of the Council;
- (d) for the category of secure integrated circuits, smart cards and related devices:
- (1) Security IC Platform PP, BSI-CC-PP-0084-2014;
  - (2) Java Card System - Open Configuration, V3.0.5 BSI-CC-PP-0099-2017;
  - (3) Java Card System - Closed Configuration, BSI-CC-PP-0101-2017;
  - (4) PP for a PC Client Specific Trusted Platform Module Family 2.0 Level 0 Revision 1.16, ANSSI-CC-PP-2015/07;
  - (5) Universal SIM card, PU-2009-RT-79, ANSSI-CC-PP-2010/04;
  - (6) Embedded UICC (eUICC) for Machine-to-Machine Devices, BSI-CC-PP-0089-2015;
- (e) for the category of points of (payment) interaction and payment terminals:
- (1) Point of Interaction "POI-CHIP-ONLY", ANSSI-CC-PP-2015/01;
  - (2) Point of Interaction "POI-CHIP-ONLY and Open Protocol Package", ANSSI-CC-PP-2015/02;
  - (3) Point of Interaction "POI-COMPREHENSIVE", ANSSI-CC-PP-2015/03;
  - (4) Point of Interaction "POI-COMPREHENSIVE and Open Protocol Package", ANSSI-CC-PP-2015/04;
  - (5) Point of Interaction "POI-PED-ONLY", ANSSI-CC-PP-2015/05;
  - (6) Point of Interaction "POI-PED-ONLY and Open Protocol Package", ANSSI-CC-PP-2015/06;

**▼B**

(f) for the category of hardware devices with security boxes:

- (1) Cryptographic Module for CSP Signing Operations with Backup - PP CMCSOB, PP HSM CMCSOB 14167-2, ANSSI-CC-PP-2015/08;
- (2) Cryptographic Module for CSP key generation services - PP CMCKG, PP HSM CMCKG 14167-3, ANSSI-CC-PP-2015/09;
- (3) Cryptographic Module for CSP Signing Operations without Backup - PP CMCSO, PP HSM CMCKG 14167-4, ANSSI-CC-PP-2015/10.

*ANNEX IV***Assurance continuity and certificate review****IV.1 Assurance continuity: scope**

1. The following requirements for assurance continuity apply to the maintenance activities related to the following:
  - (a) a re-assessment if an unchanged certified ICT product still meets its security requirements;
  - (b) an evaluation of the impacts of changes to a certified ICT product on its certification;
  - (c) if included in the certification, the application of patches in accordance with an assessed patch management process;
  - (d) if included, the review of the certificate holder's lifecycle management or production processes.
2. The holder of an EUCC certificate may request the review of the certificate in the following cases:
  - (a) the EUCC certificate is due to expire within nine months;
  - (b) there has been a change either in the certified ICT product or in another factor which could impact its security functionality;
  - (c) the holder of the certificate demands that the vulnerability assessment is carried out again in order to reconfirm the EUCC certificate's assurance associated with the ICT product's resistance against present cyberattacks.

**IV.2 Re-assessment**

1. Where there is a need to assess the impact of changes in the threat environment of an unchanged certified ICT product, a re-assessment request shall be submitted to the certification body.
2. The re-assessment shall be carried out by the same ITSEF that was involved in the previous evaluation by reusing all its results that still apply. The evaluation shall focus on assurance activities which are potentially impacted by the changed threat environment of the certified ICT product, in particular the relevant AVA\_VAN family and in addition the assurance lifecycle (ALC) family where sufficient evidence about the maintenance of the development environment shall be collected again.
3. The ITSEF shall describe the changes and detail the results of the re-assessment with an update of the previous evaluation technical report.
4. The certification body shall review the updated evaluation technical report and establish a re-assessment report. The status of the initial certificate shall then be modified in accordance with Article 13.
5. The re-assessment report and updated certificate shall be provided to the national cybersecurity certification authority and ENISA for publication on its cybersecurity certification website.

**▼B****IV.3 Changes to a certified ICT product**

1. Where a certified ICT product has been subject to changes, the holder of the certificate wishing to maintain the certificate shall provide to the certification body an impact analysis report.
2. The impact analysis report shall provide the following elements:
  - (a) an introduction containing necessary information to identify the impact analysis report and the target of evaluation subject to changes;
  - (b) a description of the changes to the product;
  - (c) the identification of affected developer evidence;
  - (d) a description of the developer evidence modifications;
  - (e) the findings and the conclusions on the impact on assurance for each change.
3. The certification body shall examine the changes described in the impact analysis report in order to validate their impact upon the assurance of the certified target of evaluation, as proposed in the conclusions of the impact analysis report.
4. Following the examination, the certification body determines the scale of a change as minor or major in correspondence to its impact.

**▼M1**

5. Where the changes have been confirmed by the certification body to be minor, no new certificate shall be issued for the modified ICT product and a maintenance report to the initial certification report shall be established.

The maintenance report shall be included as a subset of the impact analysis report, containing following sections:

- (a) introduction;
  - (b) description of changes;
  - (c) affected developer evidence.
6. The maintenance report referred to in point 5 shall be provided to ENISA for publication on its cybersecurity certification website.

**▼B**

7. Where the changes have been confirmed to be major, a re-evaluation shall be carried out in the context of the previous evaluation and by reusing any results from the previous evaluation that still apply.
8. After completion of the evaluation of the changed target of evaluation, the ITSEF shall establish a new evaluation technical report. The certification body shall review the updated evaluation technical report and, where applicable, establish a new certificate with a new certification report.
9. The new certificate and certification report shall be provided to ENISA for publication.



#### IV.4 Patch management

1. A patch management procedure provides for a structured process of updating a certified ICT product. The patch management procedure including the mechanism as implemented into the ICT product by the applicant for certification can be used after the certification of the ICT product under the responsibility of the conformity assessment body.
2. The applicant for certification may include into the certification of the ICT product a patch mechanism as part of a certified management procedure implemented into the ICT product under one of the following conditions:
  - (a) the functionalities affected by the patch reside outside the target of evaluation of the certified ICT product;
  - (b) the patch relates to a predetermined minor change to the certified ICT product;
  - (c) the patch relates to a confirmed vulnerability with critical effects on the security of the certified ICT product.
3. If the patch relates to a major change to the target of evaluation of the certified ICT product in relation to a previously undetected vulnerability having no critical effects to the security of the ICT product, the provisions of Article 13 apply.
4. The patch management procedure for an ICT product will be composed of the following elements:
  - (a) the process for the development and release of the patch for the ICT product;
  - (b) the technical mechanism and functions for the adoption of the patch into the ICT product;
  - (c) a set of evaluation activities related to the effectiveness and performance of the technical mechanism.
5. During the certification of the ICT product:
  - (a) the applicant for certification of the ICT product shall provide the description of the patch management procedure;
  - (b) the ITSEF shall verify the following elements:
    - (1) the developer implemented the patch mechanisms into the ICT product in accordance to the patch management procedure that was submitted to certification;
    - (2) the target of evaluation boundaries are separated in a way that the changes made to the separated processes do not affect the security of the target of evaluation;
    - (3) the technical patch mechanism performs in accordance with the provisions of this section and the applicant's claims;
  - (c) the certification body shall include in the certification report the outcome of the assessed patch management procedure.
6. The holder of the certificate may proceed to apply the patch produced in compliance of the certified patch management procedure to the concerned certified ICT product and shall take the following steps within 5 working days in the following cases:

**▼B**

- (a) in the case referred to in point 2(a), report the patch concerned to the certification body that shall not change the corresponding EUCC certificate;
- (b) in the case referred to in point 2(b), submit the patch concerned to the ITSEF for review. The ITSEF shall inform the certification body after the reception of the patch upon which the certification body takes the appropriate action on the issuance of a new version of the corresponding EUCC certificate and the update of the certification report;
- (c) in the case referred to in point 2(c), submit the patch concerned to the ITSEF for the necessary re-evaluation but may deploy the patch in parallel. The ITSEF shall inform the certification body after which the certification body starts the related certification activities.





## ANNEX V

### CONTENT OF A CERTIFICATION REPORT

#### V.1 Certification report

1. On the basis of the evaluation technical reports provided by the ITSEF, the certification body establishes a certification report to be published together with the corresponding EUCC certificate.
2. The certification report is the source of detailed and practical information about the ICT product or the category of ICT products and about the ICT product's secure deployment and shall therefore include all publicly available and sharable information of relevance to users and interested parties. Publicly available and sharable information can be referenced by the certification report.
3. The certification report shall at least contain the following sections:
  - (a) executive summary;
  - (b) identification of the ICT product or the ICT product category for protection profiles;
  - (c) security services;
  - (d) assumptions and clarification of scope;
  - (e) architectural information;
  - (f) supplementary cybersecurity information, if applicable;
  - (g) ICT product testing, if it was performed;
  - (h) where applicable, an identification of the certificate holder's lifecycle management processes and production facilities;
  - (i) results of the evaluation and information regarding the certificate;
  - (j) summary of the security target of the ICT product submitted to certification;
  - (k) when available, the mark or label associated to the scheme;
  - (l) bibliography.
4. The executive summary shall be a brief summary of the entire certification report. The executive summary shall provide a clear and concise overview of the evaluation results and shall include the following information:
  - (a) name of the evaluated ICT product, enumeration of the product's components that are part of the evaluation and the ICT product version;
  - (b) name of the ITSEF that performed the evaluation and, where applicable, the list of subcontractors;
  - (c) completion date of evaluation;
  - (d) reference to the evaluation technical report established by the ITSEF;
  - (e) brief description of the certification report results, including:
    - (1) the version and if applicable release of the Common Criteria applied to the evaluation;
    - (2) the Common Criteria assurance package and security assurance components including the AVA\_VAN level applied during the evaluation and its corresponding assurance level as set out in Article 52 of Regulation (EU) 2019/881 to which the EUCC certificate refers to;

**▼B**

- (3) the security functionality of the evaluated ICT product;
  - (4) a summary of threats and organisational security policies addressed by the evaluated ICT product;
  - (5) special configuration requirements;
  - (6) assumptions about the operating environment;
  - (7) where applicable, the presence of an approved patch management procedure in accordance with Section IV.4 of Annex IV;
  - (8) disclaimer(s).
5. The evaluated ICT product shall be clearly identified, including the following information:
  - (a) the name of the evaluated ICT product;
  - (b) an enumeration of the ICT product's components that are part of the evaluation;
  - (c) the version number of the ICT product's components;
  - (d) identification of additional requirements to the operating environment of the certified ICT product;
  - (e) name and contact information of the holder of the EUCC certificate;
  - (f) where applicable, the patch management procedure included into the certificate;
  - (g) link to the website of the holder of the EUCC certificate where supplementary cybersecurity information for the certified ICT product in accordance with Article 55 of Regulation (EU) 2019/881 is provided.
6. The information included in this Section shall be as accurate as possible in order to ensure a complete and accurate representation of the ICT product that can be re-used in future evaluations.
7. The security policy section shall contain the description of the ICT product's security policy and the policies or rules that the evaluated ICT product shall enforce or comply with. It shall include a reference and a description of the following policies:
  - (a) the vulnerability handling policy of the holder of the certificate;
  - (b) the assurance continuity policy of the holder of the certificate.
8. Where applicable, the policy may include the conditions related to the use of a patch management procedure during the validity of the certificate.
9. The section for the assumptions and clarification of scope shall contain exhaustive information regarding the circumstances and objectives related to the intended use of the product as referred to in Article 7(1), point (c). The information shall include the following:
  - (a) assumptions on the ICT product's usage and deployment in the form of minimum requirements, such as proper installation and configuration and hardware requirements being satisfied;
  - (b) assumptions on the environment for the compliant operation of the ICT product;

**▼B**

10. The information listed in point 9 shall be as understandable as possible in order to let users of the certified ICT product make informed decisions about the risks associated with its use.
11. The architectural information section shall include a high-level description of the ICT product and its main components in accordance with Common Criteria's ADV\_TDS subsystems design.
12. A complete listing of the ICT product supplementary cybersecurity information shall be provided in accordance with Article 55 of Regulation (EU) 2019/881. All relevant documentation shall be denoted by the version numbers.
13. The ICT product testing section shall include the following information:
  - (a) the name and point of contact of the authority or body that issued the certificate including the responsible national cybersecurity certification authority;
  - (b) the name of the ITSEF which performed the evaluation, when different from the certification body;
  - (c) an identification of the used assurance components from the standards referred by Article 3;
  - (d) the version of the state-of-the-art document and further security evaluation criteria used in the evaluation;
  - (e) the complete and precise settings and configuration of the ICT product during the evaluation, including operational notes and observations if available;
  - (f) any protection profile that has been used, including the following information:
    - (1) the author of the protection profile;
    - (2) the name and identifier of the protection profile;
    - (3) the identifier of the protection profile's certificate;
    - (4) the name and contact details of the certification body and of the ITSEF involved in the evaluation of the protection profile;
    - (5) the assurance package(s) required for a product conforming to the protection profile.
14. The results of the evaluation and information regarding the certificate section shall include the following information:
  - (a) confirmation of the attained assurance level as referred to in Article 4 of this Regulation and Article 52 in Regulation (EU) 2019/881;
  - (b) assurance requirements from the standards referred by Article 3 that the ICT product or protection profile actually meets, including the AVA\_VAN level;
  - (c) detailed description of the assurance requirements, as well as the details of how the product meets each of them;
  - (d) date of issuance and period of validity of the certificate;
  - (e) unique identifier of the certificate.

**▼B**

15. The security target shall be included in the certification report or referenced and summarised in the certification report and provided with the certification report association with it for the purposes of publication.
16. The security target may be sanitised in accordance with Section VI.2.
17. The mark or label associated to the EUCC may be inserted the certification report in accordance with the rules and procedures laid down Article 11
18. The bibliography section shall include references to all documents used in the compilation of the certification report. That information shall include at least the following:
  - (a) the security evaluation criteria, state-of-the-art documents and further relevant specifications used and their version;
  - (b) the evaluation technical report;
  - (c) the evaluation technical report for composite evaluation, where applicable;
  - (d) technical reference documentation;
  - (e) developer documentation used in the evaluation effort.
19. In order to guarantee the reproducibility of the evaluation, all documentation referred to has to be uniquely identified with the proper release date, and proper version number.

**V.2 Sanitization of a security target for publication**

1. The security target to be included in or referenced by the certification report pursuant to point 1 of Section VI.1 may be sanitised by the removal or paraphrasing of proprietary technical information.
2. The resulting sanitised security target shall be a real representation of its complete original version. This means that the sanitised security target cannot omit information which is necessary to understand the security properties of the target of evaluation and the scope of the evaluation.
3. The content of the sanitised security target shall conform to the following minimum requirements:
  - (a) its introduction shall not be sanitised as it includes no proprietary information in general;
  - (b) the sanitised security target has to have a unique identifier that is distinct from its complete original version;
  - (c) the target of evaluation description may be reduced as it may include proprietary and detailed information about the target of evaluation design which should not be published;
  - (d) the target of evaluation security environment description (assumptions, threats, organisational security policies) shall not be reduced, in so far as that information is necessary to understand the scope of the evaluation;
  - (e) the security objectives shall not be reduced as all information is to be made public to understand the intention of the security target and target of evaluation;

**▼B**

- (f) all security requirements shall be made public. Application notes may give information on how the functional requirements of the Common Criteria as referred to in Article 3 were used to understand the security target;
  - (g) the target of evaluation summary specification shall include all target of evaluation security functions but additional proprietary information may be sanitised;
  - (h) references to protection profiles applied to the target of evaluation shall be included;
  - (i) the rationale may be sanitised to remove proprietary information.
4. Even if the sanitised security target is not formally evaluated in accordance with the evaluation standards referred to in Article 3, the certification body shall ensure that it complies with the complete and evaluated security target, and reference both the complete and the sanitised security target in the certification report.



## ANNEX VI

### SCOPE AND TEAM COMPOSITION FOR PEER ASSESSMENTS

#### VI.1 Scope of the peer assessment

1. The following types of peer assessments are covered:
  - (a) Type 1: when a certification body performs certification activities at the AVA\_VAN.3 level;
  - (b) Type 2: when a certification body performs certification activities related to a technical domain listed as state-of-the-art documents in Annex I;
  - (c) Type 3: when a certification body performs certification activities above the AVA\_VAN.3 level making use of a protection profile listed as state-of-the-art documents in Annex II or III.
2. The peer-assessed certification body shall submit the list of certified ICT products that may be candidate to the review by the peer assessment team, in accordance with the following rules:
  - (a) the candidate products shall cover the technical scope of the certification body authorisation, of which at least two different products evaluations at assurance level 'high' will be analysed through the peer assessment, and one protection profile if the certification body has issued certificate at assurance level 'high';
  - (b) for a Type 2 peer assessment, the certification body shall submit at least one product per technical domain and per concerned ITSEF;
  - (c) for a Type 3 peer assessment, at least one candidate product shall be evaluated in accordance with an applicable and relevant protection profiles.

#### VI.2 Peer assessment team

1. The assessment team shall consist of at least two experts each selected from a different certification body from different Member States that issues certificates at the assurance level 'high'. The experts should demonstrate the relevant expertise in the standards as referred in Article 3 and state-of-the-art documents that are in scope of the peer assessment.
2. In the case of a delegation of certificate issuance or prior approval of certificates as referred to in Article 56(6) of Regulation (EU) 2019/881, an expert from the national cybersecurity certification authority related to the concerned certification body shall in addition participate in the team of experts selected in accordance with paragraph 1 of this Section.
3. For a Type 2 peer assessment the team members shall be selected from certification bodies being authorised for the concerned technical domain.
4. Each member of the assessment team shall have at least two years of experience of carrying out certification activities in a certification body;
5. For a Type 2 or 3 peer assessment, each member of the assessment team shall have at least two years of experience of carrying out certification activities in that relevant technical domain or protection profile and proven expertise and participation in the authorisation of an ITSEF

**▼B**

6. The national cybersecurity certification authority monitoring and supervising the peer-assessed certification body and at least one national cybersecurity certification authority whose certification body is not subject to the peer assessment shall participate in the peer assessment as an observer. ENISA may also participate in the peer assessment as an observer.
7. The peer-assessed certification body is presented with the composition of the peer assessment team. In justified cases, it may challenge the composition of the peer assessment team and ask for its review.

*ANNEX VII***Content of an EUCC Certificate**

An EUCC certificate shall at least contain:

- (a) a unique identifier established by the certification body issuing the certificate;
- (b) information related to the certified ICT product or protection profile and the holder of the certificate, including:
  - (1) name of the ICT product or protection profile and, where applicable, of the target of evaluation;
  - (2) type of ICT product or protection profile and, where applicable, of the target of evaluation;
  - (3) version of the ICT product or protection profile;
  - (4) name, address and contact information of the holder of the certificate;
  - (5) link to the website of the holder of the certificate containing the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881;
- (c) information related to the evaluation and certification of the ICT product or protection profile, including:
  - (1) name, address and contact information of the certification body that issued the certificate;
  - (2) where different from the certification body, name of the ITSEF which performed the evaluation;
  - (3) name of the responsible national cybersecurity certification authority;
  - (4) a reference to this Regulation;
  - (5) a reference to the certification report associated with the certificate referred to in Annex V;
  - (6) the applicable assurance level in accordance with Article 4;
  - (7) a reference to the version of the standards used for the evaluation, referred to in Article 3;
  - (8) identification of the assurance level or package specified in the standards referred to in Article 3 and in conformity with Annex VIII, including the assurance components used and the AVA\_VAN level covered;
  - (9) where applicable, reference to one or more protection profiles with which the ICT product or protection profile complies;
  - (10) date of issuance;
  - (11) period of validity of the certificate;
- (d) the mark and label associated with the certificate in accordance with Article 11.



*ANNEX VIII***Assurance package declaration**

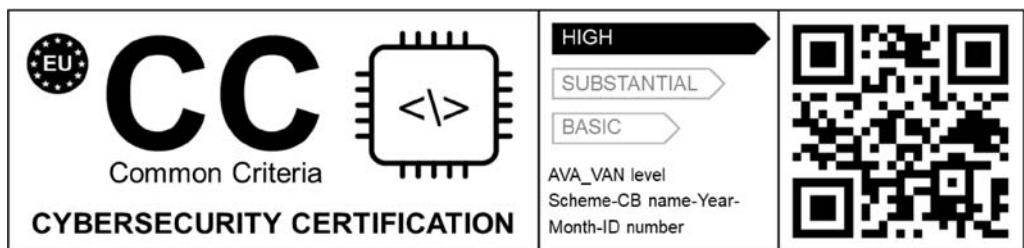
1. Contrary to the definitions in the Common Criteria, an augmentation:
  - (a) shall not be denoted by the abbreviation '+';
  - (b) shall be detailed by a list of all concerned components;
  - (c) shall be outlined in detail in the certification report.
2. The assurance level confirmed in an EUCC certificate may be complemented by the evaluation assurance level as specified in Article 3 of this Regulation.
3. If the assurance level confirmed in an EUCC certificate does not refer to an augmentation, the EUCC certificate shall indicate one of the following packages:
  - (a) 'the specific assurance package';
  - (b) 'the assurance package conformant to a protection profile' in case of referencing a protection profile without an evaluation assurance level.

▼ B

*ANNEX IX*

**Mark and label**

1. The form of mark and label:



2. If the mark and label are reduced or enlarged, the proportions given in the drawing above shall be respected.
3. Where physically present, the mark and label shall be at least 5 mm high.