EUROPEAN
COMMISSION

Brussels, XXX
[…](2023) XXX draft

**COMMISSION IMPLEMENTING REGULATION (EU) …/...**

**of XXX**

**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)



*This draft has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission.*

**COMMISSION IMPLEMENTING REGULATION (EU) …/...**

**of XXX**

**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)



THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) 526/2013 (Cybersecurity Act)[1], and in particular Article 49(7) thereof,

Whereas:

(1) This Regulation specifies the roles, rules and obligations, as well as the structure of the European Common Criteria-based cybersecurity certification scheme (EUCC) in accordance with the European cybersecurity certification framework set out in Regulation (EU) 2019/881. The EUCC builds on the Mutual Recognition Agreement ('MRA') of Information Technology Security Certificates of the Senior Officials Group Information Systems Security[2] ('SOG-IS') using the Common Criteria, including the group's procedures and documents.

(2) The scheme should be based on established international standards. Common Criteria for Information Technology Security Evaluation (ISO 15408) is an international standard for computer security evaluation. It is based on third party evaluation and envisages seven Evaluation Assurance Levels ('EAL'). The Common Criteria is accompanied by the Common Methodology for Information Technology Security Evaluation.

(3) The EUCC uses the Common Criteria's vulnerability assessment family (AVA_VAN), components 1 to 5. The five components provide all the main determinants and dependencies for analysing vulnerabilities of ICT products. As the components correspond to the assurance levels in this Regulation, they allow for a well-informed choice of assurance, based on the evaluations carried out of the security requirements and the risk associated with the intended use of the ICT product. The applicant for an EUCC certificate should provide the documentation related to the intended use of the ICT product and the analysis of the levels of risks associated with such usage in order

[1] OJ L 151, 7.6.2019, p. 15.

[2] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0 of January 2010, available on sogis.eu, approved by Senior Officials Group Information Systems Security of the European Commission in response to point 3 of Council Recommendation 95/144/EC of 7 April 1995 on common information technology security evaluation criteria (OJ L 93, 26.4.1995, p. 27–28).

to enable the conformity assessment body to evaluate the suitability of the assurance level selected.

(4) A technical domain is a reference framework that covers a group of ICT products that have specific and similar security functionality that mitigates attacks where the characteristics are common to a given assurance level. A technical domain describes in state-of-the-art documents the specific security requirements as well as additional evaluation methods, techniques and tools that apply to the certification of ICT products that are covered by this technical domain. A technical domain therefore also fosters harmonisation of the evaluation of covered ICT products. Two technical domains are currently widely used for certification at levels AVA_VAN.4 and AVA_VAN.5. The first technical domain is the 'Smart cards and similar devices' technical domain, where significant portions of the required security functionality depend on specific, tailored and often separable hardware elements (e.g. smart card hardware, integrated circuits, smart card composite products, Trusted Platform Modules as used in Trusted Computing, or digital tachograph cards). The second technical domain is 'Hardware devices with security boxes', where significant portions of the required security functionality depend upon a hardware physical envelope (referred to as a 'Security Box') that is designed to resist direct attacks, e.g. payment terminals, tachograph vehicle units, smart meters, access control terminals and Hardware Security Modules).

(5) When applying for certification, the applicant should relate its reasoning for selecting an assurance level to the objectives laid down in Article 51 of Regulation (EU) 2019/881, and to the selection of components from the catalogue of security functional requirements and security assurance requirements contained in Common Criteria. Certification bodies should assess the appropriateness of the chosen assurance level and ensure that the chosen level is commensurate with the level of risk associated with the intended use of the ICT product.

(6) Under the Common Criteria, certification is carried out against a security target which encompasses a definition of the ICT product's security problem as well as the security objectives that address the security problem. The security problem provides details on the intended use of the ICT product and the risks associated with such use. A select set of security requirements responds to both the security problem and security objectives of an ICT product.

(7) The security problem and the security requirements can also be expressed in a protection profile, as part of an ICT process supporting the development and delivery of a certified ICT product. Protection profiles are essential elements in the Common Criteria evaluation as they set out the security requirements for specific categories of ICT products. A given protection profile is used as benchmark for future security targets that fall under the given ICT product category addressed by that protection profile. Protection profiles are thus an effective means to predetermine the common cybersecurity requirements for a given category of ICT products and are therefore an essential element in the certification process of ICT products covered by the protection profile. They streamline and enhance the efficiency of the ICT product certification process and help users to specify an ICT product's functionality correctly and effectively. Protection profiles should thus be considered as integral part of the ICT process leading to the certification of ICT products.

(8) In order to enable their role as essential trustworthy and reliable benchmarks in the ICT process supporting the development and delivery of a certified ICT product,

protection profiles themselves should be able to be certified. It is therefore essential to apply at least the same level of scrutiny to protection profiles as to security targets in order to ensure a high level of cybersecurity. Protection profiles should be evaluated and certified solely by applying the Common Criteria's and Common Evaluation Methodology's assurance class for protection profiles (APE). Due to their important and sensitive role as a benchmark in the certification of ICT products, they should be certified only by public bodies or certification bodies that have received prior approval by the national cybersecurity certification authority for the certification of a specific protection profile. A protection profile should be only used in an ICT product certification process where it is published as a state-of-the-art document, including relating to technical domains, for that category of ICT products. Due to their fundamental role for certification at assurance level 'high', in particular outside of technical domains, protection profiles should be developed as state-of-the-art documents which should be endorsed by the European Cybersecurity Certification Group.

(9) Certified protection profiles should be included in the EUCC conformity and compliance monitoring by the national cybersecurity certification authorities. They should therefore also be subject to peer assessments in order to assess the methodology, tools and skills applied to the evaluation of ICT products and to be in a better position to further define technical domains based on those specific protection profiles.

(10) To achieve a high level of trust and assurance in certified ICT products, self-assessment should not be permitted under this Regulation. Only third-party conformity assessment by ITSEF and certification bodies should be allowed.

(11) The SOG-IS community harmonised the methodology for the application of the Common Criteria and the Common Evaluation Methodology in certification, in particular for the assurance level 'high' pursued by the technical domains "Smart cards and similar devices' and "Hardware devices with security boxes". The reuse of such supporting documents in the EUCC scheme ensures a smooth transition from the nationally implemented SOG-IS schemes to the harmonised EUCC scheme. Therefore, harmonised evaluation methodologies of general relevance for all certification activities should be included in this Regulation. In addition, the Commission should be able to request the European Cybersecurity Certification Group to adopt an opinion endorsing and recommending the application of evaluation methodologies specified in state-of-the-art documents for the certification of the ICT product or protection profile under the EUCC scheme. This Regulation therefore lists in Annex I the state-of-the-art documents for the evaluation activities carried out by conformity assessment bodies. A state-of-the-art document specifies evaluation methods, techniques and tools that apply to the certification of ICT products or security requirements of a generic ICT product category. The European Cybersecurity Certification Group should endorse and maintain state-of-the-art documents. State-of-the-art documents should be used in certification. Where a conformity assessment body does use them in justified cases, it should notify such non-usage with a justification to the national cybersecurity certification authority.

(12) The applicant should provide all information necessary for certification. It should be possible to reuse evaluation evidence obtained prior to the certification of an ICT product, in particular evidence relating to the sites involved in the development and production of the ICT product. Such evaluation evidence can originate from a certification process carried out under the EUCC scheme, from another European

cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881, or on the basis a national scheme referred to in Article 50 of this Regulation.

(13) The marks and labels used under EUCC aim at visibly demonstrating the trustworthiness of the certified ICT product to users and enable them to make an informed choice when purchasing ICT products. The use of marks and labels should also be subject to the rules and conditions set out in ISO/IEC 17065 and, where applicable, ISO/IEC 17030 with the applicable guidance.

(14) Certification bodies should decide on the duration of the validity of certificates taking into account the life cycle of the ICT product concerned and its necessary version management policies. The duration of the validity should not exceed five years and should be aligned with the practice in other Member States related to that ICT product.

(14a) The national cybersecurity certification authorities should monitor the developments in the field of certification by means of peer review, in accordance with Article 58(7), point (i), in conjunction with Article 59(3), point (c), of Regulation (EU) 2019/881.

(15) Where the scope of an existing EUCC certificate is reduced, a new certificate with the new scope should be issued to ensure that users are clearly informed about the current scope and assurance level of the certificate of a given ICT product.

(16) The certification of protection profiles differs from that of ICT products as it concerns an ICT process. As a protection profile covers a category of ICT products, its evaluation and certification cannot be done on the basis of a single ICT product. As a protection profile unifies the general security requirements regarding a category of ICT products and independent of the ICT product's manifestation by its vendor, the period of validity of an EUCC certificate for a protection profile should, in principle, cover five years as a minimum and may extend to the lifetime of the protection profile.

(17) Conformity assessment body is defined as a body that performs conformity assessment activities including calibration, testing, certification and inspection. However, in order to ensure a high quality of services, this Regulation specifies that calibration and testing activities should be carried out by separate entities, namely IT Security Evaluation Facilities ('ITSEF') on the one hand, and certification bodies for certification and inspection activities on the other hand. Both types of conformity assessment bodies should be accredited and, in certain situations, authorised.

(18) A certification body should be accredited in accordance with standard ISO/IEC 17065 by the national accreditation body for assurance level 'substantial' and 'high'. In addition to the accreditation in accordance with Regulation (EC) No 765/2008, conformity assessment bodies should meet specific requirements in order to guarantee their technical competence for the evaluation of cybersecurity requirements under assurance level 'high' of the EUCC, which is confirmed by an 'authorisation'. To support the authorisation process, ENISA should develop and maintain guidance and publish it after endorsement by the European Cybersecurity Certification Group.

(19) The technical competence of an ITSEF should be assessed through the accreditation of the testing laboratory in accordance with ISO/IEC 17025 and complemented by ISO/IEC 23532-1 for the full set of evaluation activities that are relevant to the assurance level and specified in ISO/IEC 18045 in conjunction with ISO/IEC 15408. Both the certification body and the ITSEF should establish and maintain an appropriate competence management system for personnel that draws from ISO/IEC 19896-1 for the elements and levels of competence and for the appraisal of

competence. For the level of knowledge, skills, experience and education, the applicable requirements for the evaluators should be drawn from ISO/IEC 19896-3. Equivalent provisions and measures dealing with deviations from such competence management systems should be demonstrated, in line with the system's objectives.

(20) In order to be authorised, the ITSEF should demonstrate its capability to determine the absence of known vulnerabilities, the correct and consistent implementation of state-of-the art security functionalities for the specific technology concerned and the targeted ICT product's resistance to skilled attackers. Additionally, for authorisations in the technical domain of 'Smart cards and similar devices', the ITSEF should also demonstrate the technical capabilities necessary for the evaluation activities and related tasks as defined in the 'Minimum ITSEF requirements for security evaluations of smart cards and similar devices'[3] supporting document under the Common Criteria. For authorisation in the technical domain 'Hardware devices with security boxes', the ITSEF should, in addition, demonstrate the minimum technical requirements necessary for carrying out evaluation activities and related tasks on hardware devices with security boxes' as recommended by the ECCG. In the context of the minimum requirements, the ITSEF should be capable of conducting the different types of attacks set out in 'Application of Attack Potential to Hardware Devices with Security Boxes' supporting document under the Common Criteria. Those capabilities encompass the evaluator's knowledge and skills and the equipment and evaluation methods needed to determine and assess the different types of attacks.

(21) The national cybersecurity certification authority should monitor the compliance of certification bodies, ITSEF and the holders of certificates with their obligations stemming from this Regulation and the Regulation (EU) 2019/881. National cybersecurity certification authority should use any appropriate sources of information to this end, including information received from certification process participants and own investigations.

(22) Certification bodies should cooperate with relevant market surveillance authorities and take into account any vulnerability information that could be relevant to ICT products for which they have issued certificates. Certification bodies should monitor certified protection profiles to identify whether the security requirements set out for a category of ICT products continue to reflect the latest developments in the threat landscape.

(23) In support of the compliance monitoring, the national cybersecurity certification authorities should cooperate with the relevant market surveillance authorities in accordance with Article 58 of Regulation (EU) 2019/881 and Regulation (EU) 2019/1020 of the European Parliament and of the Council[4]. Economic operators in the Union are obliged to share information and cooperate with market surveillance authorities, pursuant to Article 4(3) of the Regulation 2019/1020.

(24) The certification bodies should monitor the compliance of the holders of a certificate and the conformity of all certificates issued under the EUCC. The monitoring should ensure that all evaluation reports provided by an ITSEF, and the conclusions taken

[3] Joint Interpretation Library: Minimum ITSEF Requirements for Security Evaluations of Smart cards and similar devices, version 2.1 of February 2020, available at sogis.eu.

[4] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1).

therein as well as the evaluation criteria and methods are consistently and correctly applied across all certification activities.

(25) Where potential non-compliance issues are detected which affect a certified ICT product, it is important to ensure a proportional response. Certificates may therefore in a first instance be suspended. Suspension should entail certain limitations regarding the promotion and use of the ICT product in question, but not affect the validity of the certificate. Suspension should be notified to the purchasers of the affected ICT products, as well as the relevant national cybersecurity certification authority and relevant market surveillance authorities. To inform the public, ENISA should publish information about a suspension on a dedicated website.

(26) The holder of an EUCC certificate should implement necessary vulnerability management procedures and ensure that those procedures are embedded in their organisation. When becoming aware of a potential vulnerability, the holder of the EUCC certificate should perform a vulnerability analysis. Where the vulnerability analysis confirms that the vulnerability can be exploited, the certificate holder should send a report of the assessment to the certification body which should in turn inform the national cybersecurity certification authority. The report should inform about the impact of the vulnerability, the necessary changes or remedial solutions that are required including possible broader implications of the vulnerability as well as remedial solutions for other products. Where necessary, the standard EN ISO/IEC 29147 should supplement the procedure for the vulnerability disclosure.

(27) For the purpose of certification, conformity assessment bodies and national cybersecurity certification authorities obtain confidential and sensitive data and business secrets, also relating to intellectual property or compliance monitoring that require adequate protection. They should therefore have the necessary technical competencies and knowledge and should establish systems in place for the protection of information. The requirements and conditions for the protection of information should be met for both accreditation and authorisation.

(28) ENISA should provide the list of certified protection profiles on its cybersecurity certification website and indicate their status, in accordance with Regulation (EU) 2019/881.

(29) This Regulation sets out conditions for mutual recognition agreements with third countries. Such mutual recognition agreements should replace similar agreements currently in place, such as SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and Common Criteria Recognition Arrangement (CCRA).

(30) Certification bodies issuing EUCC certificates at assurance level ‘high’, as well as the relevant associated ITSEFs, should undergo peer assessments. The objective of peer assessments should be to determine the continued compliance of a peer-assessed certification body's constitution and procedures with the requirements of the EUCC scheme and, in justified cases, for the maintenance of the scheme. Peer assessments should ascertain that certification bodies work in a harmonised way and produce the same quality of certificates and they should identify any potential strength or weakness in the performance of certification bodies, also in view of sharing best practices.

(31) The European Cybersecurity Certification Group should play an important role in the maintenance of the scheme. It should, inter alia, be carried out through cooperation with the private sector, the creation of specialised subgroups and relevant preparatory work and assistance requested by the Commission. The European Cybersecurity

Certification Group plays a key role in the endorsement of state-of-the-art documents. State-of-the art documents are published in Annex I to this regulation. The Commission may amend Annex I to ensure that the list is dynamic, reflecting the opinions of the European Cybersecurity Certification Group.

(32) In a number of Member States Common Criteria certificates are issued under national schemes using mutual recognition rules established in SOG-IS MRA and CCRA. This Regulation should provide an indicative list of existing national schemes which will cease to produce effects. Member States should end their participation in the CCRA in the areas covered by this Regulation.

(33) This Regulation shall apply 12 months after its entry into force. The requirements of Chapter IV and Annex III do not require a transition period and should therefore apply as of the entry into force of this Regulation.

(34) The measures provided for in this Regulation are consistent with the opinion of the European Cybersecurity Certification Committee established by Article 66 of Regulation (EU) 2019/881,

HAS ADOPTED THIS REGULATION:

# 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 those ICT products.

*Article 2*

**Definitions**

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

(1) 'Common Criteria' mean the Common Criteria for Information Technology Security Evaluation, as set out in ISO standard EN ISO/IEC 15408;

(2) 'Common Evaluation Methodology' means the Common Methodology for Information Technology Security Evaluation, as set out in ISO standard EN ISO/IEC 18045;

(3) 'evaluation' means the determination of whether the target of evaluation's security requirements and security need as specified in a protection profile or security target are justified;

(4) '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;

(5) ‘security requirement’ means a collection of specific security functional requirements or security assurance requirements, as described in Common Criteria, that address a defined security problem and related objectives for the intended use and anticipated attack potential of a target of evaluation;

(6) ‘security need’ means a set of security requirements for the assurance of a category of ICT products;

(7) ‘security target’ means a claim of implementation-dependent security requirements for a specific ICT product;

(8) ‘protection profile’ means an ICT process that concerns the security requirements for a specific category of ICT products, addressing implementation-independent security needs, that may be used as a benchmark for certification of ICT products falling into that specific category;

(9) ‘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;

~~(10)~~ ‘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 such as calibration, testing, sampling and related inspection activities;

(11) ‘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;

(12) ‘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;

(13) ‘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;

(14) ‘national cybersecurity certification authority’ means an authority designated by a Member State pursuant to Article 58(1) of Regulation (EU) 2019/881;

(15) ‘certification body’ means a conformity assessment body as defined in Article 2 point 13 of Regulation (EC) No 765/2008, which performs only certification activities;

(16) ‘technical domain’ means a frame of reference for the harmonised certification of a group of target of evaluations with a set of required security requirements;

(17) ‘state-of-the-art document’ is 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 in order to harmonise evaluation in technical domains or of protection profiles

(18) ‘market surveillance authority’ means an authority defined in Article 3(4) of Regulation (EU) 2019/1020.

*Article 3*

**Evaluation standards**

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

(a) the Common Criteria;

(b) the Common Evaluation Methodology.

*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 VI.

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, including its documentation:

   (a) as defined by the applicant; or

   (b) incorporating a certified protection profile as part of the ICT process, where the ICT product falls into the ICT product category covered by that protection profile.

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

*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, independent functional testing and flaw remediation, 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 (2).
2. Where a conformity assessment body does not apply the relevant state-of-the-art document, it shall inform the competent national cybersecurity certification authority with a justification. The national cybersecurity certification authority shall notify such information to the European Cybersecurity Certification Group.
3. ICT product falling into a category of ICT products covered by a protection profile which has been certified as part of an ICT process and has been listed as a state-of-the-art document in Annex I, shall be evaluated in accordance with the relevant elements of that protection profile.
4. In the case of an ICT product undergoing a composite product evaluation, 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 composed ICT product.

## SECTION II

### ISSUANCE, RENEWAL AND WITHDRAWAL OF EUCC CERTIFICATES

*Article 8*

**Information necessary for certification**

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 activities.

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 to this Regulation, subject to safeguards against unauthorised disclosure.

3. Applicants for certification may provide to the certification body and ITSEF appropriate evaluation evidence 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 50 of this Regulation.

4. Where the evaluation results are pertinent to its tasks, the ITSEF shall reuse the evaluation evidence provided that such evidence conforms 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 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 10 years after the expiry of the certificate.

*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.

*Article 10*

**Content and format of an EUCC certificate**

1. An EUCC certificate shall include at least the information set out in Annex V.

2. An EUCC certificate shall unambiguously specify the scope and boundaries of the certified ICT product, 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 III 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 the certificate may affix 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 VII.

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 by digital means, the marks and labels shall visibly, legibly and indelibly appear in its documentation.

3. The mark and label as set out in Annex VII shall contain at least the following information:

   (a) the unique identification number of the certificate;

   (b) the assurance level of the certified ICT product; and

   (c) the unique identification number of the certification body that has issued the certificate.

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 III and IV;

   (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 five years.

3. By derogation from paragraph 2 that period may exceed five years, subject to the prior approval of the national cybersecurity certification authority.

*Article 13*

**Review of an EUCC certificate**

1. Where the certification body decides to review the EUCC certificate, it shall carry out such review in accordance with Annex II. 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 the EUCC certificate 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, a 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, 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, independent functional testing and flaw remediation, 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 relevant evaluation methodologies, listed as state-of-the-art documents in Annex I.

2. A protection profile may only be certified if:

   (a) it relates to a category of ICT products covered by a technical domain referred to in Annex I, in which case it shall be certified against the requirements set out in that technical domain or;

(b) it relates to a state-of-the-art document referred to in Annex I, in which case it shall be certified against the requirements set out in that document.

3. Where a conformity assessment body does not apply the relevant state-of-the-art documents, it shall inform the competent national cybersecurity certification authority with a justification. The national cybersecurity certification authority shall notify such information to the European Cybersecurity Certification Group.

## SECTION II

## ISSUING, RENEWING AND WITHDRAWING EUCC CERTIFICATES FOR PROTECTION PROFILES

*Article 16*

**Information necessary for certification 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 activities. Article 8(2), (3), (4) and (7) shall apply mutatis mutandis.

*Article 17*

**Issuance of EUCC certificates for protection profiles**

1. The applicant for certification shall provide the certification body and the ITSEF with all the necessary complete and correct information.

2. Article 9 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 security objectives of the ICT product's category covered by that protection profile.

4. A protection profile shall be certified solely by a certification body:

(a) established as a public body in accordance with Article 56(5) of Regulation (EU) 2019/881, or

(b) which has received prior approval by the national cybersecurity certification authority for the certification of that specific 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.

*Article 19*

**Review of an EUCC certificate for protection profiles**

1. Where the certification body decides to review an EUCC certificate for a protection profile, it shall carry out that review in accordance with Annex II. 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 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**

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.

# Chapter IV

# Conformity assessment bodies

*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, 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 44.

2. The national cybersecurity certification authority shall assess whether a certification body fulfils all the requirements set out in paragraph 1. This assessment shall include at least structured interviews and a review of two pilot certifications performed by the certification body.

3. The national cybersecurity certification authority shall produce an authorisation report which is subject to peer review in accordance with Article 59(3)(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 maximum of three years. It may be renewed upon request provided that the certification body still meets the requirements set out in this Article.

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 the 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, 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, its compliance 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 44.

2. The national cybersecurity certification authority shall assess whether an ITSEF fulfils all the requirements set out in paragraph 1. This assessment shall include at least structured interviews and a review of two pilot evaluations performed by the ITSEF in accordance with 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 three years at most. It may be renewed upon request provided that the ITSEF still meets the requirements set out in this Article.

5. 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.

*Article 23*

**Notification of certification bodies**

1. The national cybersecurity certification authority shall notify the Commission of the certification bodies in its territory that are competent to certify at assurance level 'substantial' based on their accreditation.

2. The national cybersecurity certification authority shall notify the Commission of the certification bodies in their territory that are competent to certify at assurance level 'high' based on their accreditation and the authorisation decision.

3. The national cybersecurity certification authority shall provide at least the following information when notifying the Commission of the certification bodies:

   (a) the assurance level or levels for which the certification body is competent to issue EUCC certificates;

   (b) the following information related to accreditation:

      (1) date of the accreditation;

      (2) name and address of the certification body;

      (3) country of registration of the certification body;

      (4) reference number of the accreditation;

      (5) scope and duration of validity of the accreditation;

      (6) the address, location and link to the relevant website of the national accreditation body; and

   (c) the following information related to authorisation for level 'high':

      (1) date of the authorisation;

      (2) reference number of the authorisation;

      (3) duration of validity of the authorisation;

      (4) scope of the authorisation including the highest AVA_VAN level and the applicable technical domain.

4. The national cybersecurity certification authority shall send a copy of the notification referred to in paragraph 1 and 2 to ENISA for the publication of accurate information on the cybersecurity certification website regarding the eligibility of certification bodies.

5. The national cybersecurity certification authority shall examine without undue delay any information regarding a change in the status of the accreditation provided by the national accreditation body. Where the accreditation or authorisation have been withdrawn, the national cybersecurity certification authority shall inform the Commission thereon, and may submit to the Commission a request in accordance with Article 61(4) of Regulation (EU) 2019/881.

*Article 24*

**Notification of ITSEF**

The notification obligations of the national cybersecurity certification authorities set out in Article 23 shall also apply to ITSEF. The notification shall include the address of the ITSEF, the valid accreditation and, where applicable, the valid authorisation of that ITSEF.

# Chapter V

# Monitoring, non-conformity and non-compliance

## SECTION I

## 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.
3. The national cybersecurity certification authority shall, in cooperation with other market surveillance authorities, sample annually at least 5% of the certified ICT products, which received certificates in the previous year from the certification bodies established in its territory. 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 II.2 of Annex II 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.

*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 an end 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.

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 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 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 Article 13, 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 19.

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 42; or

   (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 to the holder of the EUCC certificate to take remedial action.

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 and 20.

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 Article 14.

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 the 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 43(3).

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

*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 Articles 14 or 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;

   (c) where necessary, transfer the certification activities of the certification body proven to be non-compliant to another certification body.

# 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 I

## 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 and in the relevant state-of-the-art documents listed in Annex I .
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 end users and security researchers.
3. In accordance with Article 56(8) of Regulation (EU) 2019/881, the holder of an EUCC certificate shall notify the certification body that issued the EUCC certificate of any subsequently detected vulnerabilities or irregularities. The notification shall be submitted without undue delay and in any case no later than three days after having become aware of a possible vulnerability affecting the certified ICT product.
4. Where a certification body becomes aware of a vulnerability related to an ICT product for which it issued an EUCC certificate, it shall inform the holder of that certificate without undue delay and no later than three days after it became aware of the vulnerability.

*Article 34*

**Vulnerability analysis**

1. Within 90 days after having become aware of a possible vulnerability relating to its certified ICT product, the holder of an EUCC certificate shall carry out a vulnerability analysis with reference to the target of evaluation and the assurance statements contained in the certificate.
2. Where the holder of the EUCC certificate fails to carry out the vulnerability analysis within the timeframe referred to in paragraph 1, Article 30 shall apply.
3. Where the vulnerability analysis demonstrates the absence of a vulnerability, the holder of the EUCC certificate shall transmit to the certification body a substantiated summary of the results and retain the analysis for 5 years.

4. Where the vulnerability analysis confirms the existence of an exploitable vulnerability:

   (a) within the boundaries of the AVA_VAN level stated by the certificate, the holder of the certificate shall submit a vulnerability analysis report to the certification body;

   (b) beyond the boundaries of the AVA_VAN level stated by the certificate, the holder of the EUCC certificate shall transmit to the certification body a substantiated summary of the residual vulnerability and retain the analysis for 5 years.

5. 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 corresponding to the EUCC certificate shall be taken into account. The holder of the certificate may consult the ITSEF.

*Article 35*

**Vulnerability analysis report**

1. The vulnerability 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.

2. The vulnerability 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.

3. The certification body shall review the vulnerability analysis report and decide to approve or disapprove it. Where necessary, the certification body shall take into account the opinion of a competent ITSEF. Where the certification body does not approve the vulnerability analysis report, it may request further clarification. Where such clarification is not provided within a reasonable time frame, the certification body may apply Articles 14 or 29.

4. Where the vulnerability analysis report, as approved by the certification body, determines that the vulnerability can be remedied, Article 36 shall apply.

5. Where the vulnerability analysis report, as approved by the certification body, determines that the vulnerability cannot be remedied, the EUCC certificate shall be withdrawn in accordance with Article 14.

*Article 36*

**Vulnerability remediation**

1. The holder of the EUCC certificate shall submit a proposal for an appropriate remedial action to the certification body.

2. The certification body shall assess the remedial action proposed by the holder of the EUCC certificate in accordance with Annex II and shall suspend the EUCC certificate in accordance with Article 30 for the duration of the assessment.

3. Where necessary for the purposes of the assessment referred to in paragraph 2, the certification body shall request that the ITSEF perform a review of the certified ICT product.

4. The certification body shall inform the holder of the EUCC certificate of the result of the assessment referred to in paragraph 2.

5. Where, following the assessment referred to in paragraph 2, the remedial action is:

   (a) approved and implemented: the certification body shall issue a new EUCC certificate;

   (b) disapproved: the certification body may apply Article 14.

6. The existing EUCC certificate shall be withdrawn in accordance with Article 14 in both cases referred to in paragraph 5, point (a) and (b).

## SECTION II

## VULNERABILITY DISCLOSURE

*Article 37*

**Embargo period**

1. Without prejudice to any reporting obligations provided for under Union law, during the vulnerability analysis in accordance with Article 34, the holder of the EUCC certificate may impose an embargo period not exceeding 30 days, accompanied by a statement of reason, during which information on the vulnerability shall only be disclosed to the certification body that issued the certificate, the competent ITSEF, and the national cybersecurity certification authority.

2. Subject to the approval of the national cybersecurity certification authority, the holder of the EUCC certificate may extend the embargo period but not beyond the moment when absence or existence of the vulnerability is established in accordance with Article 34.

*Article 38*

**Information shared with the national cybersecurity certification authority**

1. After having received the vulnerability analysis report in accordance with Article 35, the certification body shall inform without undue delay the national cybersecurity certification authority of the confirmed vulnerability.

2. The information provided 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 applicable, any information from the certification body on the broader implications of the vulnerability for other certified ICT products.

3. The information provided in accordance with paragraph 1 shall not contain details of the means of exploitation of the vulnerability.

*Article 39*

**Cooperation with other national cybersecurity certification authorities**

1. The national cybersecurity certification authority shall share the relevant information received in accordance with Article 38 with other national cybersecurity certification authorities and ENISA.
2. Where the holder of the EUCC certificate imposed an embargo period in accordance with Article 37, the national cybersecurity certification authority shall share the relevant information at the end of the embargo period.
3. 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 40*

**Publication of the vulnerability**

Upon withdrawal of the certificate pursuant to Article 36(6), the holder of the EUCC certificate shall disclose and register any publicly known vulnerability in the ICT product on the European vulnerability database, established in accordance with Article 12 of Directive (EU) 2022/2555 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 41*

**Retention of records by certification bodies and ITSEF**

1. 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 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 expiry of the relevant EUCC certificate.

*Article 42*

**Information made available by the holder of the 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 end-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 expiry of the relevant EUCC certificate:

(a) records of the information provided to the certification body and to the ITSEF during the certification process; and

(b) specimen of the certified ICT product.

3. 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 43*

**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 44;

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 the EUCC certificate.

*Article 44*

**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 preserving intellectual property rights, and take the necessary and appropriate technical and organisational measures.

# Chapter VIII

# Mutual recognition agreements with third countries

*Article 45*

**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 a monitoring and supervising 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;

   (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 46*

**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 IV.

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 48 specifies which results were reused with or without further assessment;

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 IV.

*Article 47*

**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. The phase of the site visit to the certification body shall last at least two weeks. During that 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 such factors as the possibility of reusing existing peer assessment evidence and results or on the number of ITSEF and technical domains the certification body issues certificates for.

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 that address the findings.

*Article 48*

**Peer assessment report**

1. The peer assessment team shall provide the peer-assessed body with a draft of the peer assessment report.

2. The peer-assessed 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.

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 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 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 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 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 peer assessment report and all relevant documents.

# Chapter X

# Maintenance of the scheme

*Article 49*

**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.

# Chapter XI

# Final provisions

*Article 50*

**National schemes covered by the EUCC**

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 one year after the entry into force of this Regulation, including the following national cybersecurity certification schemes in-so-far as they apply to the evaluation standards referred to in Article 3 and the specific evaluation criteria and methods referred to in Article 6:

(1) Orden PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (Spain),

(2) Ordinance with instructions for the Swedish Defence Materiel Administration: Förordning med instruktion för Försvarets materielverk (SFS 2007:854) (Sweden),

(3) Appropriation Directions for the Swedish Defence Material Administration: Regleringsbrev avseende Försvarets materielverk (Sweden),

(4) Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG), § 9 (1), (2) und (4) (Germany),

(5) Décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information (France),

(6) Decreto del Presidente del consiglio dei ministri 30 ottobre 2003, 'Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'Art. 10, comma 1, del decreto legislativo 23 febbraio 2002, n. 10.' (GU n. 98 del 27-04-2004) (Italy),

(7) Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging (NSCIB), version 2.5, dated 28-03-2019 (Netherlands),

(8) Pismo wyznaczające Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy do wypełniania zadań uczestnika kwalifikowanego w ramach porozumień SOG-IS oraz CCRA, reference number DC.WRCiS.1106.7.2022, dated 2022/03/30 (Poland)

*Article 51*

**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 12 months after the entry into force.

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

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

Done at Brussels,

*For the Commission*
*The President*
*Ursula VON DER LEYEN*