EUROSMART
The Voice of the Digital Security Industry

Executive Summary of Eurosmart's Feedback on the Draft EUCC Implementing Act

Eurosmart welcomes the European Commission's proposed amendments to the EU Cybersecurity Certification Scheme on Common Criteria (EUCC). While broadly supportive of the objectives, Eurosmart identifies several areas where clarification and adjustments seem to be necessary to ensure practicality, and alignment with existing practices:

1. Definition of Major Changes

- Current definition only covers negative impacts. Eurosmart recommends extending it to any significant change - positive or negative -that affects assurance.

2. Security Target Publication

- Only **sanitised versions** of security targets should be made publicly available. This ensures consistency with Annex V of Implementing Regulation 2024/482 and protects sensitive information.

3. Application of State-of-the-Art (SotA) Documents

- It must be clear that SotA documents applicable only if published before the start of an evaluation. Once an evaluation started, the version in force should apply to avoid rework and inconsistencies.

4. Clarity on Protection Profiles (PPs)

- **Annex II** should explicitly list *mandatory PPs* (at AVA_VAN.4 or 5), while **Annex III** should clearly cover *recommended PPs*. Eurosmart calls for clarification on whether Annex III PPs must become EUCC-certified or recognised SotA documents.

5. Re-Assessment and Patch Management

- The re-assessment process must clearly define outcomes: either confirmation or modification of assurances, depending on results.

- Patch handling procedures should clarify when a new certificate is (or is not) issued, ensuring alignment between Annex IV provisions and Article 13/19 of the Regulation.

6. Annex V: Intended Use and Certification Reporting

- Requirements for intended use should be more **specific and less subjective**, to ensure clear understanding across all stakeholders.

- Certification bodies should not be burdened with summarising vulnerability management procedures; instead, certificate holders should provide publicly available information in line with Article 8(b).

EUROSMART
The Voice of the Digital Security Industry

Name: Eurosmart [1] [2] comments on Draft EUCC Implementing Act

Date: 2025-08-28

Document: EUCC Implementing Act

Name #[1]	Article	Type of comment[2]	Comments	Proposed change
Eurosmart	Art 1 (1) (18)	te	Major change provision for products that have negative impact, this should apply to main changes that either positively or negatively that impact the assurance that can be expected.	(18) 'major change' means any change in the certified target of evaluation or its environment that may ~~adversely~~ impact the assurance expressed in the EUCC certificate.';
Eurosmart	Recital 12 Art 1(6)(b) Art 1(6)(a)	te	This provision amends Article 42: the security target should be provided to ENISA. However, a sanitised version of the security target should only be provided together with the certification report (as per Annex V, Section VI.2 of Implementing regulation 2024/482). More generally, it should be clarified that whenever publication of the security target is required, it must be the sanitised version.	(6) Article 42 is amended as follows: (a) in paragraph 1, the following point (i) is added: '(i) the **sanitised** security target corresponding to each EUCC certificate, **according to Annex V.2.** (b) paragraph 2 is replaced by the following: 'The information referred to in paragraph 1 shall be made available at least in English. For that purpose, certification bodies shall provide ENISA with the original language versions of the certification reports and **sanitised** security targets, **according to Annex V.2,** and in addition they shall also provide the English version of such documents without undue delay.';
Eurosmart	Art 1(7)	ge	We understand the amendment as follow: only the State-of-the-Art (SotA) documents with an applicability date prior to the start date of a certification process, re-evaluation or re-evaluation must be taken into account. Once an evaluation process has begun - with the registration completed and an Evaluation Technical Report (ETR) under preparation - the version of the EUCC Implementing Regulation in force at the date of initiation should apply. Otherwise, some tasks should be repeated in order to comply with newly introduced rules and SotA documents.	
Eurosmart	Annex I (b)(5)	te	Hardware assessment in EN 419221-5 (HSM PP)", version 1; This document is not a Protection Profile (PP) as such, we recommend putting the full title of the document	Replace by **(5) Hardware assessment in EN 419221-5 (HSM PP): interpretation of the FPT_PHP requirements, Version 1, February 2025**

EUROSMART
The Voice of the Digital Security Industry

Name: Eurosmart [1] [2] comments on Draft EUCC Implementing Act

Date: 2025-08-28

Document: EUCC Implementing Act

Name #[1]	Article	Type of comment[2]	Comments	Proposed change
Eurosmart	Annex II	te	Our understanding is that Annex II lists the mandatory Protection Profiles (PPs), while Annex III lists the recommended ones, as provided in Article 7(1)(e) and recitals 9 and 31 of Implementing Regulation (EU) 2024/482, published in the OJEU.	Modify the title of Annex II: **Mandatory** Protection profiles certified at AVA_VAN level 4 or 5
Eurosmart	Annex II and Annex III	ge	Distinction between mandatory (Annex II) and recommended (Annex III) should be better explained - Open questions: - Are Annex II mandatory PPs necessarily EUCC certified? - Are Annex III PPs to necessarily become EUCC certified PPs in the future and/or become recognised SotA documents?	Provide clearer explanations in recitals of the Implementing Regulation (EU) 2024/482
Eurosmart	Annex III and I		"Others: Trusted Execution Environment Protection Profile – GPD_SPE_021 (v1.3), ANSSI-CC-PP-2014/01-M02.' " and ANNEX 3 is entitled "Recommended protection profiles (illustrating technical domains from Annex I)". This protection profile is at assurance level AVA_VAN.2 + AVA_VAN_TEE, corresponding to the assurance level "substantial" according to the regulation Regulation (EU) 2019/881. Annex I lists state of the art documents supporting technical domains for VAN.4 and VAN.5. Does it mean that state of the art documents supporting technical domains at "substantial" will be included in Annex I ? Moreover, Annex III includes several PPs with assurance level not compliant to Regulation (EU) 2019/881, such as the POI ones. is it planned to update those protection profiles to make them compliant?	in case the answer is yes, recommend adding Annex I is amended as: **"3. State-of-the-art documents supporting technical domains at substantial:** **[BLANK] "**
Eurosmart	Annex IV.1	ge	re-assessment is defined in Annex IV.2: it is a change in the threat environment of the TOE and the ITSEF will check the impact of that change on the assurance claimed/stated by the certificate, that is a check that the	Modify as it follows "4. If the re-assessment process is successful, **no impact on the assurances stated by the certificate**, Article 13 paragraph 2 points (a) or (c) applies in the case of the certification of a

Name #[1]	Article	Type of comment[2]	Comments	Proposed change
			TOE is still robust or not, the security control (SFR + SAR) are still enough to mitigate that new threat.	product and Article 19 paragraph 2 point (a) or (c) applies in the case of the certification of a protection profile. If the re-assessment process is not successful**, the assurances stated by the certificate is modified**, Article 13 paragraph 2 point (b) or (d) applies in the case of the certification of a product and Article 19 paragraph 2 point (b) or (d) applies in the case of the certification of a protection profile"
Eurosmart	ANNEX IV.3, 5.		According to IV.4, 6. (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;" and IV.4, 2. (b) "the patch relates to a predetermined minor change to the certified ICT product" this means that the "appropriate action" using ANNEX IV.3, 5. of the CB will confirm the change as minor, in accordance to Article 13 2. (a), the certificate will be confirmed and then **no new certificate** will be issued. in case this interpretation is correct, i.e. no new version of the certificate will be issued, it is recommended to add the reference to IV.4, 6. (b)	IV.4, 6. (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, **in accordance with Article 13 paragraph 2 point (a) or Article 19 paragraph 2 point (a)** , on the issuance of a new version of the corresponding EUCC certificate and the update of the certification report.
Eurosmart	Annex V:	ge	Annex V introduces the notion of **intended use of the product**, aiming to align with the CRA. Wording improvement needed : - Requirements should be less subjective and directly understandable**.** (e.g. Annex VI part 8 last paragraph is highly interpretative: *The information referred to in the first subparagraph shall be as **clear and understandable** as possible to enable potential users of the certified ICT product to make informed decisions about the risks associated with its use*).	Recommendation: provisions should be **more specific and less subjective** to ensure broader understanding and compliance.

Name #[1]	Article	Type of comment[2]	Comments	Proposed change
			- This could be acceptable to experienced EUCC stakeholders but unclear for new participants (e.g., new issuing countries, new customers).	
Eurosmart	ANNEX V.3(c) & 6(b)	ge	ANNEX V.3(c) &6(b) introduces "the name of the developer" and "name and contact information of the holder of the EUCC certificate" as two information for (3)"the contact information related to the evaluation of the ICT product" , does this later refers to the contact for vulnerability disclosure/notification referred to in chapter VI ? A product could be developed in several development sites, therefore "name of the developer" may be a list of development sites, which one to mention in the certification report ?	Proposal for Annex V.1 6 (a) "name of the developer **as stated in the security target**"
Eurosmart	ANNEX V.3(d) and (7)		the certification report established by the certification body should include (3) (d) "security policies" (7) that the evaluated product shall enforce or comply with. "It shall also include "(a) a description of the vulnerability management and vulnerability disclosure procedures of the certificate holder, to be completed solely with information that can be made publicly available" it may be complex for the CB to summarize the description of the vulnerability management and disclosure procedures of the certificate holder, i.e. identifying without the support of the certificate holder, the information that can be made publicly available. Therefore (a) could refer to the public information provided by the certificate holder according to the article 8 (b) of the regulation Implementing Regulation (EU) 2024/482.	" 7. The security policy referred to in paragraph 3, point (d), shall contain the description of the ICT product's security policy as a collection of security services and the policies or rules that the evaluated ICT product shall enforce or comply with. It shall also include the following information: (a) a description of the vulnerability management and vulnerability disclosure procedures of the certificate holder, **provided according to Article 8 (b),** to be completed solely with information that can be made publicly available; "