EUROSMART
The Voice of the Digital Security Industry

Eurosmart's comments

Draft implementing regulation establishing the European cybersecurity certification scheme (EUCC) based on Common Criteria (CC)

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13382-Cybersecurity-security-requirements-for-ICT-product-certification_en

Introduction

Eurosmart and its members are delighted to be able to contribute to the implementation of the first European certification scheme. This initial scheme underscores the rigor and technical expertise of common criteria in Europe, an area in which Eurosmart and its members have been active contributors for many years.

The release of this implementing regulation represents a substantial stride towards a more cyber-resilient Europe. While commending the efforts of the Commission, the Member States, and ENISA, Eurosmart also wishes to provide constructive feedback for the scheme's practical implementation.

Eurosmart has categorized its feedback into two parts. The first part highlights elements deemed highly critical, requiring necessary modifications. The second part focuses on elements that Eurosmart believes should receive additional technical implementation clarifications. Moreover, Eurosmart encourages the legislator to pay special attention to the following points:

1. Mutual recognition

International recognition remains a significant uncertainty for many stakeholders, whilst international recognition is essential for businesses. Member States should uphold mutual recognition rules, particularly the Common Criteria Recognition Arrangement (CCRA), until the European Union Cybersecurity Certification (EUCC) has an equivalent agreement with international communities. Additionally, the text does not include provisions for recognizing Protection Profiles (PP) that have been recognized outside the EU (as mentioned on the CC portal).

2. Transitional period and SOG-IS transposition

In line with the Cybersecurity Act, the text envisions an abrupt termination of national schemes, while some certificates may remain valid. The management of these certificates remains unresolved. The current text does not explicitly outline a clear transposition procedure. Eurosmart advocates for a 2-year grace period remains a transitional solution and does not resolve the issue of mutual recognition.

Within 2 years, SOGIS certificates must be transitioned into EUCC certificates. The question that remains is how the transposition of SOGIS and the implementation of the EUCC will simplify and enhance the efficiency of certifications within the already extensively employed technical domains, where there is a significant demand for such streamlining.

3. Monitoring Activities and Other Additional Efforts under Chapter V

Many provisions are described that will result in additional efforts for Certification Authorities (CABs) and Information Technology Security Evaluation Facilities (ITSEFs). The text does not specify who will bear these costs.

4. Scheme Maintenance

There are few references to scheme maintenance in the text. An ad-hoc working group from ENISA (TG-M) has developed an ISAC (Information Sharing and Analysis Centre) proposal to ensure the continuity of Joint Interpretation Library Working Groups (JIL-WGs). The recitals in the current text only refer to subgroups within ECCG by technical domains. Limiting it to such an approach might not be very neither encouraging for the in-depth involvement of private stakeholders, nor stimulating an efficient collaboration between public and private actors.

5. List of SOTA Documents

The implementing act refers to dynamic documents initiated by the ECCG. However, by referencing a certain number of documents in the annex of this act, their legal updates become exceedingly complex. Furthermore, the list of Protection Profiles (PPs) does not appear to be up to date. Will future PPs require a new delegated act to be referenced?

Part I.

Summary of the review - critical issues

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
(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 Co mmission.	Clarification needed	The ECCG is tasked with the endorsement of SOTA documents through cooperation with the private sector, and the creation of specialised subgroups (within the ECCG?). The wording could be misleading. Does it mean that the ECCG directly liaise with the private sector and host future technical groups? Is an ISAC as an interface to facilitate exchanges between public and private still an option?	**Recommended edit:** 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 public-private technical working groups**, the creation of specialised subgroups and relevant preparatory work and assistance requested by the Commission.
(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.	Critical issue	This means there is no transition period in which certificates can be issued under both the EUCC and the National Schemes. See also the CSA Article 57 (1): [...]National cybersecurity certification schemes, and the related procedures for the ICT products, ICT services and ICT processes that are covered by a European cybersecurity certification scheme **shall cease to produce effects from the date established in the implementing act adopted pursuant to Article 49(7).** [...]	It would be more practical not to allow new applications in the National Schemes, when the EUCC Scheme starts. A grace period should allow the handling of issuesof the already existing certifications, and the finish of the ongoing evaluations which may not comply the rules of EUCC. This big bang approach could impact vendors' trust of Common Criteria International recognition are mandatory for the business. Member States should be able to current maintain mutual recognition rules, mainly CCRA, until EUCC will not have an equivalent agreement with international communities. The following proposal to extend to 2 years remains a transitional solution and does not resolve the issue of mutual recognition. Within 2 years, SOGIS certificates must be transitioned into EUCC certificates. As a reminder, SOGIS certificates are valid until the end of their lifespan, but there are no longer schemes to manage them. **Recommended edits:**
(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.	Critical issue		
Art. 50	**Chapter XI Final provisions** *Article 50 National schemes covered by the EUCC* In accordance with the CSA Article 57 1 and 3, **national cybersecurity certification schemes and the related**	Critical issue		

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	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. (List of schemes are provided)			(32) [...] This Regulation should provide an indicative list of existing national schemes which will cease to produce effects **after a transition period of 24 months.** (33) This Regulation shall apply **24** months after its entry into force **Art 50.** In accordance with the CSA Article 57 1 and 3, national cybersecurity certification schemes and the related procedures for ICT products and ICT processes that are covered by the EUCC shall cease **to receive new applications** from **two** years after the entry into force of this Regulation.
Art. 2	**Chapter I General provisions** *Article 2 Definitions* (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 […] ISO standard **EN ISO/IEC 18045;**	Critical issue	This can re-introduce the copyright issue which had been solved by also referring to the CCRA CC:2022 version	We understand that the EN has been adopted, so a European legislation should not refer to the Common Criteria any other ways just as an EN, but it is important also to handle the copyright issues which arose when Common Criteria copyrights have been handed to ISO.
Art. 7(3)	*Chapter II Certification of ICT products SECTION I SPECIFIC STANDARDS AND REQUIREMENTS FOR EVALUATION* *Article 7 Evaluation criteria and methods for ICT products*	Critical issue	This means that if there is an EUCC approved PP for a product, it can be only certified according to that PP. What about to non-EU PP that are registered on the CC portal?	This approach is limiting. It should be allowed to also use other criteria as well. Instead of shall, use should. **Recommended edits:**

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	(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.**			(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**~~ ***should*** be evaluated in accordance with the relevant elements of that protection profile.
Art. 7(1)(d)	*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: […] **(d) the applicable state-of-the-art documents listed in Annex I (2).**	Clarification needed or typo	There is no (2) part of the Annex I.	
Recital (8)	*(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****…*	Clarification needed		
Art. 8(3) (4)	*SECTION II - ISSUANCE, RENEWAL AND WITHDRAWAL OF EUCC CERTIFICATES* *Article 8 Information necessary for certification*	Clarification needed	That means the developers shall receive the evaluation reports in its entirety, and can share with other CABs?	Please clarify how the sharing of the prior evaluation evidence is possible without infringement of copyright/NDAs.

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	3. Applicants for certification may provide to the certification body and ITSEF appropriate evaluation evidence from **prior certification** 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.**			
Art. 9(1)(a)	*Article 9 Conditions for issuance of an EUCC certificate* 1. (a) CB and ITSEF accredited/authorised **for the category of the ICT products**	Clarification needed	These types and categories are currently not available. Are we refering to a taxonomy / a list of product to be covered by the CRA?	Clarification of ICT product catergories and types is necessary to fully interpret the EUCC implementing act. As taxonomy is important to understand the IA, we propose to put it into an Annex, or if that is not possible, make it available during the review of the implementing act.
Art. 21	*Article 21 Additional or specific requirements for a certification body* The national cybersecurity certification authority **shall specify the ICT product categories and protection profiles** to which the authorisation extends	Clarification needed		
Art. 22 (4)	*Article 22 Additional or specific requirements for the ITSEF* 4. The national cybersecurity certification authority shall specify the **ICT product categories** and protection profiles to which the authorisation extends.	Clarification needed		
Annex V	*ANNEX V: Content of an EUCC Certificate*	Clarification needed		

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	(2) type of ICT product and, where applicable, of the target of evaluation;			
Art.12	*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.**	Critical issue	Each NCCA could decide on a prolongation, by doing so, it would create discrepancies instead of harmonisation. Moreover, it contradicts the approach of recital (14) that provides: - *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*	Delete point 3 of article 12 or approval need to be done at ECCG level. Recommended edits: 3. By derogation from paragraph 2 that period may exceed five years, subject to the prior approval of the ~~***national cybersecurity certification authority***~~ ***European Cybersecurity Certification Group***.
Art. 20	*Withdrawal of an EUCC certificate for a PP*	Critical issue	What is the impact on certified products with a dedicated PP when this PP is withdrawn? What is the impact on the renewal of certificate ? maintenance etc…	Proposal: To clarify the process of PP certification. Use the same process that used today by SOGIS
Art. 19	*Article 19* *Review of an EUCC certificate for protection profiles* **CB can request the ITSEF to perform a re-evaluation of PP**	Clarification needed	Who will afford these additional efforts?	Clarification is needed on the status of additional workloads related to CABs, which are not initiated by Certificate holders, see also Article 27.2 What is exactly the definition of "monitoring compliance which task need to be done? why the selection is done on "product which received certificates in the previous year?
Art. 25(3)	*Article 25* *Monitoring activities by the national cybersecurity certification authority* 3) **The national cybersecurity certification authority national**	Clarification needed		

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	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 NCCA, **certification bodies and, if necessary, ITSEF shall assist that authority in monitoring compliance.**			
Art. 25(6)	(6) The **certification body**that certified the sampled ICT product shall, upon request of the NCCA, with the **assistance of the respective ITSEF, conduct additional review**	Clarification needed		
Art. 31(b)	*Article 31 Consequences of non-compliance by the conformity assessment body* 1. In case of non-compliance by a certification body with its obligations, or by the relevant certification body in case of identifying non-compliance by an ITSEF, the national cybersecurity certification authority shall, without undue delay: [...] b) where necessary, request evaluation activities to be performed on TOE or PP, either by the ITSEF which performed the	Clarification needed		

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	evaluation, or any other ITSEF that may be in a better technical position to support that identification			
Art. 36(3)	*Article 36 Vulnerability remediation* 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**	Clarification needed		
Art 31(2)(a) and (b)	*Article 31 Consequences of non-compliance by the conformity assessment body* 1. In case of non-compliance by a certification body with its obligations, or by the relevant certification body in case of identifying non-compliance by an ITSEF, the national cybersecurity certification authority shall, without undue delay: (a) identify, with the support of the concerned ITSEF, the potentially affected EUCC certificates; (b) where necessary, request evaluation activities to be performed on one or more ICT products or protection profiles by either the ITSEF which performed the evaluation, or any other accredited and,	Clarification needed	If this is the non-compliance of the CB, how come that the CB can decide the action? What's the rational for such a decision? Could a CAB decide alone? This approach would be detrimental to the European harmonisation.	The handling of the non-compliance by the conformity assessment body opens the door to mismanadgement and liability issues. Instead of the CB, the NCCA shall have the powers listed to handle the non-compliance. **Recommended edits:** 2. On the basis of the measures referred to in paragraph 1, the certification body **under supervision of the NCCA** shall adopt either of the following decisions with respect to each affected EUCC certificate:

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	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.			
Art. 35(3)	*Article 35 Vulnerability analysis report* 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	Critical issue	There are no reciprocity in the timeframes, the NCCAs, CBs and ITSEFS should also have timeframes. Also, related to Article 362., there is a compulsory suspension of the certificate during the duration of the CB assessment, which should not be the case.	CSA, and the EUCC is voluntary, but there are timelines from other obligatory regulations (Like CRA) and there is a need to align to those as well. All parties shall follow the strict timelines, not just the holders of certificates, as there are also other legislation in other ICT domains and those also need to be followed **Recommended edits:** 2. The certification body shall assess the remedial action proposed by the holder of the EUCC certificate

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	clarification. **Where such clarification is not provided within a reasonable time frame,** the certification body may suspend or withdraw the certificate			in accordance with Annex II and shall suspend the EUCC certificate in accordance with Article 30 for the duration of the assessment, **if necessary.**
Art. 36	*Article 36 Vulnerability remediation* 1. The Holder of the certificate submits its proposal for an appropriate remedial action 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**	Critical issue		
Art. 39(1)	*Article 39 Cooperation with other national cybersecurity certification authorities* 1. After NCCA received the vulnerability analysis report, **it shall share with other National Cybersecurity Certification Authorities and ENISA.**	Critical issue	The sharing of the Vulnerability Analysis Report shall be limited to the affected NCCAs, and the text shall indicate this	The sharing of data is very vague in the EUCC implementing act, there is no understanding of how the sharing should work, and it is hard to agree on the text as it no precision. Sharing should be on a need-to-know basis. Also, this regulation about the sharing does not indicate any timelines at all, while it should Recommended edits: 1. After NCCA received the vulnerability analysis report, it shall share with other ***affected*** National cybersecurity Certification Authorities and ENISA **on a need to know basis**.

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
Art. 40	*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	Critical issue	That means that the vulnerability shall be only disclosed after the Certificate is withdrawn	Any other changes to the certificate, like scope reduction shall also trigger the Vulnerability disclosure process. **Recommended edits:** Upon ***the issuance of a new EUCC Certificate pursuant to Article 36(5)(a) or*** withdrawal of the certificate pursuant to Article ***36(5)(a) or*** 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
Art. 21 (c)	*Article 21 Additional or specific requirements for a certification body* (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'**	Clarification needed	What is the penalty of non-conformance? Who is auditing the compliance of this?	We welcome the inclusion of the protection of information into the EUCC Implementing act, but it needs more precison, like indications of auditing the compliance to this requirement, and also consequences of non-compliance
Art. 44	*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.**	Clarification needed		

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
Art.45	*Mutual recognition agreements with third countries – Conditions*		MRA is critical for the quick implementation and the good functionning of the EUCC.	In order to manage a smooth transition, the same kind of agreement done between the Member States and CCRA should apply.
Art. 50	**Chapter XI Final provisions** *Article 50 National schemes covered by the EUCC* 1. In accordance with the CSA Article 57 1 and 3, **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**. (List of schemes are provided)	Critical issue	This means that there is no transition period. SOGIS certificates stay available until end of validity. If SOGIS Scheme no longer exist how these certificates will be managed? There is no information about transposition of certificate, how a SOGIS Certificate will be transposed on EUCC Certificate	A clear mechanism should be defined in the delegated act providing a transition period.
Annex I	**List of PPs**	Critical issue	The list of PPs referenced in Annex I is not complete. Some major SOGIS certified PPs are missing, meaning that EUCC cannot be used by industry relying on these PPs. Recital 11 provides that the list is dynamic. However as these SOTA documents are listed in annex of a Commission implementing regulation, the update of such a document requires a comitology process. It highly complexify slow down the adoption of updated SOTA documents.	Recommandation: Create a real dynamic list and simplify the administrative process. Annex I as a dynamic list should not be part of the implementing regulation. A dynamic list including all the necessary PPs should be published as a dinctinct document, placed on a online portal under the responsability of the Commission and maintained by the ECCG. The implementing regulation should refer to this list. This list sould be published on a portal under the responsability of the ECCG and the Commission.
Recital 31	**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.**			

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
Annex II.2	*ANNEX II: Assurance continuity* *II.2 Re-assessment* 4. The certification body shall review the updated evaluation technical report and establish a re-assessment report. The status of the initial certificate shall then be modified in accordance with the following outcomes of the re-assessment activities: (a) continuation of the EUCC certificate without changes to the assurance level: when the target of evaluation was found conformant to the AVA_VAN component as previously claimed in the security target, the validity of the previous certificate shall be extended by no more than 5 years; (b) continuation of the EUCC certificate with changes to the assurance level: when the target of evaluation was not found conformant to the AVA_VAN component as previously claimed in the security target, the certificate shall be altered only for the new AVA_VAN level reached by the re-assessed target of evaluation. The previous certificate shall be archived.	Clarification needed	This is not that simple, what happens with the PP claims for example?	The re-assessment case (b) above can end up to noncompliance to the PP, the ST needs to be changed as well, the and the certificate should be clear that any compliance to PPs are removed. That should be part of the text to be clear. **Recommended edits:** b) continuation of the EUCC certificate with changes to the assurance level: when the target of evaluation was not found conformant to the AVA_VAN component as previously claimed in the security target, the certificate shall be altered only for the new AVA_VAN level reached by the re-assessed target of evaluation. The previous certificate shall be archived. ***If this effects to noncompliance to the previously referenced PP, the ST shall be changed, and the references to the PPs in the certificate shall be removed.***
Annex III.2.3 (f)	*ANNEX III: Content of a certification report*	Critical issue	In the original document CCDB-2006-04-004 ST sanitising for publication: *All security requirements have to be made public. Application notes might give*	Refinements and application notes sanitazation should be allowed in the Annex, as it is also allowed for other CCRA locations.

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	III.2 Sanitization of a security target for publication 3. The content of the sanitised security target shall conform to the following minimum requirements: (f) all security requirements shall be made public. Application notes may give information on how the functional requirements of the Common Criteria as referred to in Article 3 were used to understand the security target;		*information on how CC Part 2 components were used to understand the ST*. However, refinements and application notes might be sanitized to remove proprietary information (e.g. about design).	**Recommended edits:** (f) all security requirements shall be made public. Application notes may give information on how the functional requirements of the Common Criteria as referred to in Article 3 were used to understand the security target, ***refinements and application notes might be sanitized to remove proprietary information (e.g. about design).;***

Part II.

Full of the review

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
Recital (20)	(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.	Clarification needed	**Question**: Is there a list of specific technologies? (Not in the Implementing Act or its Annexes)	Clarification of ICT product catergories and types is necessary to fully interpret the EUCC implementing act. As taxonomy is important to understand the IA, we propose to put it into an Annex, or if that is not possible, make it available during the review of the implementing act.
Recital (25)	(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.***	Clarification needed	Does this indicate that the purchasers of the ICT products need to be documented? Does this mean that ENISA need to create a dedicated website about Certificate suspensions?	
Recital (32)	(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	Critical issue	See above.	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	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.			
Recital (33)	(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.	Critical issue	This means there is no transition period in which certificates can be issued under both the EUCC and the national schemes. See also the CSA Article 57 (1): "[...]National cybersecurity certification schemes, and the related procedures for the ICT products, ICT services and ICT processes that are covered by a European cybersecurity certification scheme **shall cease to produce effects from the date established in the implementing act adopted pursuant to Article 49(7).** [...]"	
Art. 2	**Chapter I General provisions** *Article 2 Definitions* (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 […] ISO standard **EN ISO/IEC 18045;**	Critical issue	This can re-introduce the copyright issue which had been solved by also referring to the CCRA CC:2022 version. Why is ~~(10)~~ crossed out?	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	~~(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;			
Art. 5	**Chapter I General provisions** *Article 5 Methods for certifying ICT products* 1. Certification of an ICT product shall be carried out **against its security target**, including its documentation. 2. Protection profiles shall be certified for the sole purpose of the certification of ICT products falling into the specific category of ICT products.	Wording	Strangely formulated. It is surely not just against the security target.	
Art. 7	**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 […] shall, as a minimum, be evaluated in accordance with the following:	Critical issue	**Referring to point 1:** How is (b) more than (a)? Why is it added? **Referring to point 3:** This means that if there is an EUCC approved PP for a product, it can be only certified according to that PP. See also above.	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	(a) applicable elements of CC and CEM; **(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[...] (d) the applicable state-of-the-art documents. 2. Where a conformity assessment body does not apply the relevant state-of-the-art document, it shall […] justify. 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.**			
Art. 8 (1) (2) (3) (4) (6) (7)	**Chapter II Certification of ICT products 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	Critical issue	**Referring to point 2**: Currently in the CC:2022 part 3 10.4.3: Source code or hardware diagrams and/or IC hardware design language code or layout data that are used to build the actual hardware are examples of parts of an implementation representation. It is important to note that while **the implementation representation must be made available to the evaluator,**	Consistency about the retention periods should be achieved.

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	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 […]** 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.		**this does not imply that the evaluator needs to possess that representation.** – this interpretation is important and should not be changed because of the new EUCC IA.. **Referring to point 3:** That means the developers shall receive the evaluation reports in its entirety, and should be able to share with other evaluators... **Referring to point 4:** Does this mean interchange of evaluation evidence in between ITSEFs? (Theoretically that is already the case, see "2002-08-009 Reuse of Evaluation Results and Evidence"). about this point, see above. **Referring to point 6:** Is there a requirement related to this procedure? **Referring to point 7**: All other places indicate 5 years, see: - Article 34 (3) and (4) (b). - Article 41 2. - Article 42.2	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	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.**			
Art. 9	**Chapter II Certification of ICT products SECTION II ISSUANCE, RENEWAL AND WITHDRAWAL OF EUCC CERTIFICATES**	Comment	**Refering to point (a)** These categorisation or taxonomy for the ICT products are currently not available.	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	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; **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;**		**Refering to point (b)** From our knowledge; previously, certificate holders were not committed to such commitments.	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	(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.**			
Art. 10 (2)	**Chapter II Certification of ICT products SECTION II ISSUANCE, RENEWAL AND WITHDRAWAL OF EUCC CERTIFICATES** *Article 10 Content and format of an EUCC certificate* ***1.*** *An EUCC certificate shall include at least the information set out in Annex V. EU certificate shall specify the scope and boundaries of the certified*	Comment	**Referring to point 2:** This is also important for CRA, where the CRA requires the certification of the full product.	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	ICT product, EU certificate shall specify the scope and boundaries of the certified ICT product, indicating whether the ***entire ICT product has been certified or only parts thereof.*** *indicating whether the* ***entire ICT product has been certified or only parts thereof.***			
Art. 19	**Chapter III Certification of protection profiles** **SECTION II - ISSUING, RENEWING AND WITHDRAWING EUCC CERTIFICATES FOR PROTECTION PROFILES** *Article 19 Review of an EUCC certificate for protection profiles* PP certs can be also reviewed by a CB according to Assurance Continuity. CB can request the ITSEF to perform a re-evaluation of PP. Results can be the same as for products.	Critical issue	CB can request the ITSEF to perform a re-evaluation of PP – but who pays for this? See also above	
Art. 20	*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	Clarification needed	What is the impact on certified products with a dedicated PP when this PP is withdrawn?	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	that issued that certificate. Article 14 shall apply mutatis mutandis.			
Art. 21	**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 (b) it conducts its certification activities in cooperation with an ITSEF (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'**.	Clarification needed	What is the actual requirement here, and what are penalties if the CB/ITSEF is nonconformant?	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
Art. 22	**Chapter IV Conformity assessment bodies** *Article 22 Additional or specific requirements for the ITSEF* [...] 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.	Critical issue	What are the categories? It is unknown as of now. Also see above	
Art. 25	**Chapter V Monitoring, non-conformity and non-compliance** **SECTION I COMPLIANCE MONITORING** *Article 25 Monitoring activities by the national cybersecurity certification authority* 1 [...]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	Clarification needed	Referring to point 3: Who pays for this sampling and the assistance? Referring to point 6:Also, who is covering the costs of these additional review? Referring to point 7: What are investigations?	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	authority, certification bodies and, if necessary, ITSEF shall assist that authority in monitoring compliance. [...] 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.			
Art. 26	**Chapter V Monitoring, non-conformity and non-compliance** **SECTION I COMPLIANCE MONITORING** *Article 26 Monitoring activities by the certification body* [...] 3. The national cybersecurity certification authority may draw up rules for a	Clarification needed	What is the form of this dialogue, and what are the possible consequences?	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	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.			
Art. 27	**Chapter V Monitoring, non-conformity and non-compliance** **SECTION I COMPLIANCE MONITORING** *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,	Clarification needed	Is this the coverage of the costs? According to the review it is not payment, just the sharing of information, please clarify what this support means.	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	the national cybersecurity certification authority to support their monitoring activities.			
Art. 28	**Chapter V Monitoring, non-conformity and non-compliance** **SECTION II CONFORMITY AND COMPLIANCE** *Article 28 Consequences of non-conformity of a certified ICT product or protection profile* **[...]** 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	Clarification needed	Clarification is needed about the sentence. Example of such a case?	
Art. 29	**Chapter V Monitoring, non-conformity and non-compliance**	Clarification needed	What is the difference in between 2 and 3 penalty if both are penalties ?	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	SECTION II CONFORMITY AND COMPLIANCE *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.			
Art. 30	**Chapter V Monitoring, non-conformity and non-compliance - SECTION II CONFORMITY AND COMPLIANCE**	Clarification needed	Clarification/Guidance is needed about the determination of sensitive information/security risk?	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	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.[...]			
Art. 31	**Chapter** *Article 31 Consequences of non-compliance by the conformity assessment body*	Clarification needed	See above	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	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**			

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	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.			
Art. 33	**Chapter VI Vulnerability management and disclosure** **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 laid down in this Section and, supplemented by the procedures set out in **EN ISO/IEC 30111 and in the relevant state-of-the-art documents.** 2. The holder of an EUCC certificate shall maintain and publish appropriate methods for receiving information on vulnerabilities related to their products; 3. Holder of EUCC certificate shall notify the CB of any **subsequently detected vulnerabilities** or irregularities. The	Comment/ Clarification needed	**Referring to point 1 (Comment):** ISO 30111 does not include certification procedures. There are no relevant state of the art documents related to Vulnerability management procedures in the Annex. **Referring to point 2 and 3:** The two highlighted parts in yellow in points 2 and 3 don't match. First part is about subsequently detected vulnerabilities or irregularities, second part is about possible vulnerabilities. **Referring to point 4:** Here we have reciprocity, we shall have that at other places as well.	**Recommended edits:** 4. Where a certification body becomes aware of ***subsequently detected vulnerabilities or irregularities*** 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 ***possible*** vulnerability.

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	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.			
Art. 34	**Chapter VI Vulnerability management and disclosure** **SECTION I VULNERABILITY MANAGEMENT** *Article 34 Vulnerability analysis* [...] 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. 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	Clarification needed	**Referring to point 3:** Only a substantiated summary is needed to be sent. Clarification is needed about the contents of the substantiated summary. **Referring to point 5:** This means that the Attack Potential calculation is done by the vendor, who MAY consult the ITSEF about it. How is it ensured that the holders of certificates have the necessary expertise to correctly calculate the Attack potentials? Also, there are no state of the art documents listed in the Annex I related to Vulnerability Management.	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	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.			
Art. 35	**Chapter VI Vulnerability management and disclosure** **SECTION I VULNERABILITY MANAGEMENT** *Article 35 Vulnerability analysis report* 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	Clarification needed/Critical issue	**Referring to point 2:** Limited distribution parties are not defined,maybe they should be. **Referring to point 3:** There are no reciprocity in the timeframes, the NCCAs, CBs and ITSEFS should also have timeframes. See above also **Referring to point 3**: Who pays for the efforrt of the ITSEF to create an opinion ? **Referring to point 3**: Reasonable timeframe is also not defined.	**Recommended edits:** 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 to ***the certification body who issued the original certificate***. 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 ***preferably the one who evaluted the product for the original certification.*** 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, ***if necessary;*** (b) disapproved: the certification body may apply Article 14.

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	frame, the certification body may apply Articles 14 or 29.			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), ***except if there was no need to issue a new certificate.***
Art. 36	**Chapter VI Vulnerability management and disclosure** **SECTION I VULNERABILITY MANAGEMENT** *Article 36 Vulnerability remediation* 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. CB Informs the holder of the certificate of the result of the assessment mentioned in 2. 5. (a) if the remedial action is approved and implemented, the 5. Where, following the assessment referred to in paragraph 2, the remedial action is:	Clarification needed/Critical issue	**Referring to point 2:** The duration of the CB assessment of the vulnerability analysis report shall be defined. **Referring to point 2:** There should be a timeline indication for the duration of the assessment, as the certificate is suspended during this. Also see above There is also a question of the identity of the ITSEF performing this review, Which ITSEF can do such assessment? **Referring to point 5 and 6**: What if there is a case where the remedial action does not need to concern the scope of the certificate? In that case why withdraw and issue a new certificate?	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	(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).**			
Art. 37	**Chapter VI Vulnerability management and disclosure** **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	Clarification needed	**Referring to point 1:** Not compulsory, but needs a statement of reason. To whom does this need to be sent, and does it need acceptance from the party? **Referring to point 2:** According to our interpretation that is the moment the Vulnerability report is available.	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	period **but not beyond the moment when absence or existence of the vulnerability is established in accordance with Article 34.**			
Art. 38	**Chapter VI Vulnerability management and disclosure** **SECTION II VULNERABILITY DISCLOSURE** *Article 38 Information shared with the national cybersecurity certification authority* 1. After receiving the vulnerability analysis report, the CB shall inform the NCCA **of the confirmed vulnerability;** 2.	Comment	The CB only needs to inform the NCCA about the confirmed vulnerability!	
Art. 39	**Chapter VI Vulnerability management and disclosure** **SECTION II VULNERABILITY DISCLOSURE** *Article 39 Cooperation with other national cybersecurity certification authorities* After NCCA received the vulnerability analysis report, it 1. After NCCA received the vulnerability analysis report, **it shall share with other National Cybersecurity Certification Authorities and ENISA.**	Critical issue	The sharing of the Vulnerability Analsis Report shall be limited to the affected NCCAs, and the text shall indicate this. See also above	The sharing of data is very vague in the EUCC implementing act, there is no understanding of how the sharing should work, and it is hard to agree on the text as it no precision. Sharing should be on a need-to-know basis. Also, this regulation about the sharing does not indicate any timelines at all, while it should **Recommended edits:** 1. After NCCA received the vulnerability analysis report, it shall share with other ***affected* national** cybersecurity certification authoritiesand ENISA ***on a need to know basis***.
Art. 40	**Chapter VI Vulnerability management and disclosure**	Critical issue	This means that the vulnerability shall be only disclosed after the Certificate is withdrawn	Any other changes to the certificate, like scope reduction shall also trigger the Vulnerability disclosure process.

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	SECTION II VULNERABILITY DISCLOSURE *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.		See also above	**Recommended edits:** Upon **the issuance of a new EUCC Certificate pursuant to Article 36(5)(a) or** withdrawal of the certificate pursuant to Article **36(5)(a) or** 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
Art. 41	**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.	Comment	This means only electronic archival system is possible in relation to EUCC.	
Art. 42	**Chapter VII Retention, disclosure and protection of information** *Article 42 Information made available by the holder of the certificate* 1. The information referred to in Article 55 of CSA shall be available in a **language that can be easily accessible to end-users;**	Clarification needed/comment	**Referring to point 1:** Language that can be easily accessible to end-usersis not defined, probably based on the market of the product, English surely needs to be accepted, but this formulation of the requirement is vague **Referring to point 2**: 1 specimen of the product – previously this was not a requirement	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	2. The holder of the certificate shall store for at least 5 years after the EU Cer is expired: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.**			
Art. 43	**Chapter VII Retention, disclosure and protection of information** *Article 43 Information to be made available by ENISA* 1. ENISA needs to publish: 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;	Comment/ Clarification needed	**Referring to point 1 f:** The reference should be Article 48 instead of 44. **Referring to point 3:** How can „without delay" be correctly interpreted?	**Recommended edits:** (h) peer assessment reports issued in accordance with Article **48**;

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	(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;** 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).			
Art. 44	**Chapter VII Retention, disclosure and protection of information** *Article 44 Protection of information*	Critical issue	What is the penalty of non-conformance? Who is auditing the compliance of this? Also see above.	We welcome the inclusion of the protection of information into the EUCC Implementing act, but it needs more precison, like indications of auditing the

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	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.			compliance to this requirement, and also consequences of non-compliance
Art. 45	**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.	Clarification needed	**Referring to point 1:** How is this interpreted in relation of the CCRA, where the schemes ceasing to exist already have a mutual recognition agreement?	
Art. 46	**Chapter IX Peer assessment of certification bodies** *Article 46 Peer assessment procedure* 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,	Clarification needed	The indication that the peer-assessment can only be done on-site in a legal document, makes it impossible to deal with special circumstances, like the COVID.to	**Recommended edits:** 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, ***except if the ECCG approves otherwise.***

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	peer assessments shall be performed on-site.			
Art. 47	**Chapter IX Peer assessment of certification bodies** Article 47 Peer assessment phases 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.	Comment	According to expierence 2 weeks of site visit is too much of burden at both sides. Even manufacturing site visits do not last more than a week.	**Recommended edits:** *2. The phase of the site visit to the certification body shall last at least **a day per assessed certification or evaluation cases** . 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.*
Art. 48	**Chapter IX Peer assessment of certification bodies** Article 48 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.** 5. The European Cybersecurity Certification Group shall adopt an opinion on the peer assessment report: (a) Where the peer-assessment	Critical issue	**Referring to point 2:** What if there are no findings? Add: if applicable. **Referring to point 5(a):** What are all relevant documents? Specific list is needed. **Referring to point 5(b):** Note, this is the only penalty, and this might even not be a good idea, as the findings might contain vulnerabilities on handling of information..	**Recommended edits:** 2. The peer-assessed body shall submit to the peer assessment team comments regarding the findings **if applicable** and a list of commitments to address the shortcomings identified in the draft peer assessment report, **if applicable.** (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, **except if there are parts which needs to be omitted based on the requirement of protection of information.**

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	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.**			
Art. 49	**Chapter IX Maintenance of the scheme** *Article 49 Maintenance of the EUCC* 1. The Commission may request the ECCG to adopt an opinion in view of maintaining the EUCC and to undertake the necessary preparatory works. 2. The ECCG may adopt an opinion to endorse state-of-the-art documents. 3. State-of-the-art documents which have	Clarification needed	How do these change and become part of the Implementing Act? Can these be changed without the endorsement of the Commission?	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	been endorsed by the European Cybersecurity Certification Group **shall be published by ENISA.**			
Art. 51	**Chapter XI Final provisions** *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.	Critical issue	This means there is no transition period in which certificates can be issued under both the EUCC and the National Schemes.	**Recommended edits:** It shall apply ~~12~~ **24** months after the entry into force.
Annex I	**Annex I: State of the Art Documents** List of applicable state of the art documents	Clarification needed	Note that there is no versioning for the state of the art documents, but there is versioning for the PPs listed. That should be uniform. For the state of the art documents the Annex I contains Mandatory documents and one trial use document: 'Certification of "open" smart card products' – why? For the list of PPs, the SOGIS webpage indicates the following: **"This webpage has not been maintained since beginning of 2019; see the CCRA PP list for the last updated PPs"**	**Recommended edits:** - 1(c)(b)(4) PP for a Secure Signature Creation Device - Part 5: Extension for device with key generation and trusted communication with signature creation application, **BSI-CC-PP-0072-2012-MA-01**; - 1(c)(b)((5) PP for a Secure Signature Creation Device - Part 6: Extension for device with key import and trusted communication with signature creation application, **BSI-CC-PP-0076-2013-MA-01**; **- 1(c)(d)(7) PP for Embedded UICC for Consumer Devices, BSI-CC-PP-0100-2018**

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
			This results in some important PPs not in the list, like: Embedded UICC for Consumer Devices Protection Profile, BSI-BSI-CC-PP-0100-2018 just to add an example. This, together with the fact that Article 7 3. requires the usage of the listed PPs, makes it important to review the list of PPs with the support of the industry experts. On the SOGIS webpage, there are also interpretations of PPs, like: - *JIL QSCD Certification Interpretation* - *JIL Clarification of tachograph Motion sensor PP* Why are these not included? The following two identifications are mixed: - 1(c)(b)(4) PP for a Secure Signature Creation Device - Part 5: Extension for device with key generation and trusted communication with signature creation application, BSI-CC-PP-0076-2013-MA-01; - 1(c)(b)((5) PP for a Secure Signature Creation Device - Part 6: Extension for device with key import and trusted communication with signature creation application, BSI-CC-PP-0072-2012-MA-01;	

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
Annex II	**Annex II: Assurance continuity** *II.2 Re-assessment* 4. (b) continuation of the EUCC certificate with changes to the assurance level: when the target of evaluation was not found conformant to the AVA_VAN component as previously claimed in the security target, **the certificate shall be altered only for the new AVA_VAN level reached by the re-assessed target of evaluation. The previous certificate shall be archived.**	Critical issue	This is not that simple, what happens with the PP claims for example? See also above	The re-assessment case (b) above can end up to noncompliance to the PP, the ST needs to be changed as well, the and the certificate should be clear that any compliance to PPs are removed. That should be part of the text to be clear. **Recommended edits:** b) continuation of the EUCC certificate with changes to the assurance level: when the target of evaluation was not found conformant to the AVA_VAN component as previously claimed in the security target, the certificate shall be altered only for the new AVA_VAN level reached by the re-assessed target of evaluation. The previous certificate shall be archived. ***If this effects to noncompliance to the previously referenced PP, the STshall be changed, and the references to the PPs in the certificate shall be removed.***
Annex II	**Annex II: Assurance continuity** *II.3 Changes to a certified ICT product* *4. Following the examination, the certification body determines the scale of a change as minor or major in correspondence to its impact. ENISA may publish guidelines as referred to in Article **46(2), point (d),** of this Regulation on its cybersecurity certification website in accordance with Article 50 of Regulation (EU) 2019/881.*	Clarification needed	Referring to point 2: The contents listed does not contain the updated evidences, just the description of evidence modifications. Referring to pint 4: IA Article 46(2) does not have (d).	**Recommended edits:** 2. The impact analysis report shall provide the following elements: (a) an introduction containing necessary information to identify the impact analysis report and the target of evaluation subject to changes; (b) a description of the changes to the product; (c) the identification of affected developer evidence;

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
				(d) a description of the developer evidence modifications; (e) the findings and the conclusions on the impact on assurance for each change. (f) updated evidence related to the changes
Annex II	**Annex II: Assurance continuity** *II.4 Patch management* 1. A patch management procedure provides for a structured process of updating a certified ICT product. The patch management procedure including the mechanism as implemented into the ICT product by the applicant for certification can be used after the certification of the ICT product **under the responsibility of the conformity assessment body.** 3. If the patch relates to a major change to the target of evaluation of the certified ICT product in relation to a previously undetected vulnerability having no critical effects to the security of the ICT product, the provisions of **Article 18 apply.**	Clarification needed	**Referring to point 1:** It is not clearwhy is this the responsibility of the conformity assessment body? **Referring to point 2:** This is good, as major change should be Assurance continuity. **Referring to point 3:** Article 18 Period of validity of an EUCC certificate for protection profiles - this is erroneous reference	
Annex III	**Annex III: Content of a certification report** *III.1 Certification report* 3. **(c) Security services**	Clarification needed	Looking at the list of the content in point 3. (c) Security services – Should be rather Security policy Point 6 refers to:	Recommended edits: 3 (c) Security ~~services~~ **policy**

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	6. The information included **in this Section** shall be as accurate as possible in order to ensure a complete and accurate representation of the ICT product that can be re-used in future evaluations.		6. The information included in this Section shall be as accurate as possible in order to ensure a complete and accurate representation of the ICT product. But it is not clear what section it refers to.	
Annex III	**Annex III: Content of a certification report** *III.2 Sanitization of a security target for publication* (f) all security requirements shall be made public. **Application notes may give information on how the functional requirements of the Common Criteria as referred to in Article 3 were used to understand the security target.**	Critical issue	In the original document CCDB-2006-04-004 ST sanitising for publication: - All security requirements have to be made public. Application notes might give information on how CC Part 2 components were used to understand the ST. However, refinements and application notes might be sanitized to remove proprietary information (e.g. about design). Refinements and application notes sanitazation should be allowed in the Annex. Also see above	Refinements and application notes sanitazation should be allowed in the Annex, as it is also allowed for other CCRA locations. **Recommended edits:** (f) all security requirements shall be made public. Application notes may give information on how the functional requirements of the Common Criteria as referred to in Article 3 were used to understand the security target,**refinements and application notes might be sanitized to remove proprietary information (e.g. about design).;**
Annex IV	**Annex IV: Scope and team composition for peer assessments** *IV.1 Scope of the peer assessment* 1. Peer assessment types: (a) Type 1: when a certification body performs certification activities at the AVA_VAN.3 level; (b) Type 2: when a certification body performs certification activities related to	Clarification needed	**Referring to point 1(b):** Should be Article 15. **Referring to point 1(c):** Should be Article 15.	**Recommended edits:** (b) Type 2: when a certification body performs certification activities related to a technical domain referred to in Article **15**(2), point (a); c) Type 3: when a certification body performs certification activities above the AVA_VAN.3 level making use of a protection profile published as a state-of-the-art document referred to in Article **15**(2), point (b).

Article/ Recital	Original European Commission's proposal or common understanding	Type of comment	Interpretation and potential issues	Proposal / Recommended edits
	a technical domain referred to in Article 6(2), point (a); c) Type 3: when a certification body performs certification activities above the AVA_VAN.3 level making use of a protection profile published as a state-of-the-art document referred to in **Article 6(2), point (b).**			
Annex V	**Annex V: Content of an EUCC Certificate** **(2) type of ICT product and, where applicable, of the target of evaluation.**	Clarification needed	The applicable types are not available. Also see above.	Clarification of ICT product catergories and types is necessary to fully interpret the EUCC implementing act. As taxonomy is important to understand the IA, we propose to put it into an Annex, or if that is not possible, make it available during the review of the implementing act.
Annex VI	**Annex VI: Assurance package declaration** Contrary to the definitions in the Common Criteria, an augmentation: **(a) shall not be denoted by the abbreviation '+';**	Clarification needed	What is the reason for this? This denotion is used for a long time.	

With more than 25 years of experience, Eurosmart gathers technological experts in the field of the Digital security. We advocate for a high security level in digital interactions.

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 2 895 36 56 | mail contact@eurosmart.com