EUROPEAN
COMMISSION

Brussels, XXX
[…](2023) XXX draft

ANNEXES 1 to 7

ANNEXES

to the

COMMISSION IMPLEMENTING REGULATION

laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)

ANNEX I: State-of-the-art documents

1. The following documents are considered as state-of-the-art documents:

   (a) documents related to the harmonised evaluation of technical domain 'smart cards and similar devices' and in particular the following documents:

      (1) 'Minimum ITSEF requirements for security evaluations of smart cards and similar devices';

      (2) 'Minimum Site Security Requirements';

      (3) 'Application of Common Criteria to integrated circuits';

      (4) 'Security Architecture requirements (ADV_ARC) for smart cards and similar devices';

      (5) 'Certification of "open" smart card products';

      (6) 'Composite product evaluation for smart cards and similar devices';

      (7) 'Application of Attack Potential to Smartcards';

   (b) documents related to the harmonised evaluation of technical domain 'hardware devices with security boxes' and in particular the following documents:

      (1) 'Minimum ITSEF requirements for security evaluations of hardware devices with security boxes';

      (2) 'Minimum Site Security Requirements';

      (3) 'Application of Attack Potential to hardware devices with security boxes';

   (c) protection profiles used in certification of ICT products falling under the below stated ICT product category:

      (a) for the category of passports:

         (1) PP Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011-MA-01;

         (2) PP for a Machine Readable Travel Document with "ICAO Application" Extended Access Control, , BSI-CC-PP-0056-2009;

         (3) PP for a Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE, BSI-CC-PP-0056-V2-2012-MA-02;

         (4) PP for a Machine Readable Travel Document with "ICAO Application" Basic Access Control, BSI-CC-PP-0055-2009;

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

         (1) PP for a Secure Signature Creation Device - Part 2: Device with key generation, BSI-CC-PP-0059-2009-MA-02;

         (2) PP for a Secure Signature Creation Device - Part 3: Device with key import, BSI-CC-PP-0075-2012-MA-01;

         (3) PP for a Secure Signature Creation Device - Part 4: Extension for device with key generation and trusted communication with certificate generation application, BSI-CC-PP-0071-2012-MA-01;

(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 ;

(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;

(c) for the category of digital tachographs:

(1) Digital Tachograph - Tachograph Card, BSI-CC-PP-0091-2017;

(2) Digital Tachograph - Vehicle unit, BSI-CC-PP-0094-2017;

(3) Digital Tachograph - External GNSS Facility (EGF PP), BSI-CC-PP-0092-2017;

(4) Digital Tachograph - Motion Sensor (MS PP), BSI-CC-PP-0093-2017;

(d) for the category of secure integrated circuits, smart cards and related devices:

(1) Security IC Platform PP, BSI-CC-PP-0084-2014;

(2) Java Card System - Open Configuration, BSI-CC-PP-0099-2017;

(3) Java Card System - Closed Configuration, BSI-CC-PP-0101-2017;

(4) PP for a PC Client Specific Trusted Platform Module Family 2.0 Level 0 Revision 1.16, ANSSI-CC-PP-2015/07;

(5) Universal SIM card, ANSSI-CC-PP-2010/04;

(6) Embedded UICC (eUICC) for Machine-to-Machine Devices, BSI-CC-PP-0089-2015;

(e) for the category of points of (payment) interaction and payment terminals:

(1) Point of Interaction "POI-CHIP-ONLY", ANSSI-CC-PP-2015/01;

(2) Point of Interaction "POI-CHIP-ONLY and Open Protocol Package", ANSSI-CC-PP-2015/02;

(3) Point of Interaction "POI-COMPREHENSIVE", ANSSI-CC-PP-2015/03;

(4) Point of Interaction "POI-COMPREHENSIVE and Open Protocol Package", ANSSI-CC-PP-2015/04;

(5) Point of Interaction "POI-PED-ONLY", ANSSI-CC-PP-2015/05;

(6) Point of Interaction "POI-PED-ONLY and Open Protocol Package", ANSSI-CC-PP-2015/06;

(f) for the category of Hardware Security Modules:

(1) Cryptographic Module for CSP Signing Operations with Backup - PP CMCSOB, ANSSI-CC-PP-2015/08;

(2) Cryptographic Module for CSP key generation services - PP CMCKG, ANSSI-CC-PP-2015/09;

(3) Cryptographic Module for CSP Signing Operations without Backup - PP CMCSO, ANSSI-CC-PP-2015/10.

ANNEX II: Assurance continuity

II.1 Assurance continuity: scope

1. The following requirements for assurance continuity apply to the maintenance activities related to the following:

   (a) a re-assessment if an unchanged certified ICT product still meets its security requirements;

   (b) an evaluation of the impacts of changes to a certified ICT product on its certification;

   (c) if included in the certification, the application of patches in accordance with an assessed patch management process.

2. The holder of an EUCC certificate may request the review of the certificate in the following cases:

   (a) the EUCC certificate is due to expire within nine months;

   (b) there has been a change either in the certified ICT product or in another factor which could impact its security functionality;

   (c) the holder of the certificate demands that the vulnerability assessment is carried out again in order to to reconfirm the EUCC certificate's assurance associated with the ICT product's resistance against present cyberattacks..

II.2 Re-assessment

1. Where there is a need to assess the impact of changes in the threat environment of an unchanged certified ICT product, a re-assessment request shall be submitted to the certification body.

2. The re-assessment shall be carried out by the same ITSEF that was involved in the previous evaluation by reusing all its results that still apply. The evaluation shall focus on assurance activities which are potentially impacted by the changed threat environment of the certified ICT product, in particular the relevant AVA_VAN family and in addition the assurance lifecycle (ALC) family where sufficient evidence about the maintenance of the development environment shall be collected again.

3. The ITSEF shall describe the changes and detail the results of the re-assessment with an update of the previous evaluation technical report.

4. The certification body shall review the updated evaluation technical report and establish a re-assessment report. The status of the initial certificate shall then be modified in accordance with 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.

5. The re-assessment report and updated certificate shall be provided to the national cybersecurity certification authority and ENISA for publication on its cybersecurity certification website.

II.3 Changes to a certified ICT product

1. Where a certified ICT product has been subject to changes, the holder of the certificate wishing to maintain the certificate shall provide to the certification body an impact analysis report.

2. The impact analysis report shall provide the following elements:

   (a) an introduction containing necessary information to identify the impact analysis report and the target of evaluation subject to changes;

   (b) a description of the changes to the product;

   (c) the identification of affected developer evidence;

   (d) a description of the developer evidence modifications;

   (e) the findings and the conclusions on the impact on assurance for each change.

3. The certification body shall examine the changes described in the impact analysis report in order to validate their impact upon the assurance of the certified target of evaluation, as proposed in the conclusions of the impact analysis report.

4. Following the examination, the certification body determines the scale of a change as minor or major in correspondence to its impact. 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.

5. Where the changes have been confirmed by the certification body to be minor, a new certificate shall be issued for the modified ICT product and a maintenance report to the initial certification report shall be established, under following conditions:

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

      (1) introduction;

      (2) description of changes;

      (3) affected developer evidence;

   (b) the validity date of the new certificate shall not exceed the date of the initial certificate.

6. The new certificate including the maintenance report shall be provided to ENISA for publication on its cybersecurity certification website.

7. Where the changes have been confirmed to be major, a re-evaluation shall be carried out in the context of the previous evaluation and by reusing any results from the previous evaluation that still apply.

8. After completion of the evaluation of the changed target of evaluation, the ITSEF shall establish a new evaluation technical report. The certification body shall review the updated evaluation technical report and, where applicable, establish a new certificate with a new certification report in accordance with Article 13 and 16.

9. The new certificate and Certification Report shall be provided to ENISA for publication.

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.

2. The applicant for certification may include into the certification of the ICT product a patch mechanism as part of a certified management procedure into the ICT product under one of the following conditions:

   (a) the functionalities affected by the patch reside outside the target of evaluation of the certified ICT product;

   (b) the patch relates to a predetermined minor change to the certified ICT product;

   (c) the patch relates to a confirmed vulnerability with critical effects on the security of the certified ICT product.

3. If the patch relates to a major change to the target of evaluation of the certified ICT product in relation to a previously undetected vulnerability having no critical effects to the security of the ICT product, the provisions of Article 18 apply.

4. The patch management procedure for an ICT product will be composed of the following elements:

   (a) the process for the development and release of the patch for the ICT product;

   (b) the technical mechanism and functions for the adoption of the patch into the ICT product;

   (c) a set of evaluation activities related to the effectiveness and performance of the technical mechanism.

5. During the certification of the ICT product:

   (a) the applicant for certification of the ICT product shall provide the description of the patch management procedure;

   (b) the ITSEF shall verify the following elements:

      (1) the developer implemented the patch mechanisms into the ICT product in accordance to the patch management procedure that was submitted to certification;

      (2) the target of evaluation boundaries are separated in a way that the changes made to the separated processes do not affect the security of the target of evaluation;

      (3) the technical patch mechanism performs in accordance with the provisions of this section and the applicant’s claims;

   (c) the certification body shall include in the certification report the outcome of the assessed patch management procedure.

6. The holder of the certificate may proceed to apply the patch produced in compliance of the certified patch management procedure to the concerned certified ICT product and shall take the following steps within 5 working days in the following cases:

(a) in the case referred to in point 2(a), report the patch concerned to the certification body that shall not change the corresponding EUCC certificate;

(b) in the case referred to in point 2(b), submit the patch concerned to the ITSEF for review. The ITSEF shall inform the certification body after the reception of the patch upon which the certification body takes the appropriate action on the issuance of a new version of the corresponding EUCC certificate and the update of the certification report;

(c) in the case referred to in point 2(c), submit the patch concerned to the ITSEF for the necessary re-evaluation but may deploy the patch in parallel. The ITSEF shall inform the certification body after which the certification body starts the related certification activities.

ANNEX III: Content of a certification report

III.1 Certification report

1. On the basis of the evaluation technical reports provided by the ITSEF, the certification body establishes a certification report to be published together with the corresponding EUCC certificate.

2. The certification report is the source of detailed and practical information about the ICT product or the category of ICT products and about the ICT product's secure deployment and shall therefore include all publicly available and sharable information of relevance to users and interested parties. Publicly available and sharable information can be referenced by the certification report.

3. The certification report shall at least contain the following sections:

   (a) executive summary;

   (b) identification of the ICT product or the ICT product category for protection profiles;

   (c) security services;

   (d) assumptions and clarification of scope;

   (e) architectural information;

   (f) supplementary cybersecurity information, if applicable;

   (g) ICT product testing, if it was performed;

   (h) results of the evaluation and information regarding the certificate;

   (i) summary of the security target of the ICT product submitted to certification;

   (j) when available, the mark or label associated to the scheme;

   (k) bibliography.

4. The executive summary shall be a brief summary of the entire certification report. The executive summary shall provide a clear and concise overview of the evaluation results and shall include the following information:

   (a) name of the evaluated ICT product, enumeration of the product's components that are part of the evaluation and the ICT product version;

   (b) name of the ITSEF that performed the evaluation and, where applicable, the list of subcontractors;

   (c) completion date of evaluation;

   (d) reference to the evaluation technical report established by the ITSEF;

   (e) brief description of the certification report results, including:

      (1) the version and if applicable release of the Common Criteria applied to the evaluation;

      (2) the Common Criteria assurance package and security assurance components including the AVA_VAN level applied during the evaluation and its corresponding assurance level as set out in Article 52 of Regulation (EU) 2019/881 to which the EUCC certificate refers to;

      (3) the security functionality of the evaluated ICT product;

(4) a summary of threats and organisational security policies addressed by the evaluated ICT product;

(5) special configuration requirements;

(6) assumptions about the operating environment;

(7) where applicable, the presence of an approved patch management procedure in accordance with Section II.4 of Annex II;

(8) disclaimer(s).

5. The evaluated ICT product shall be clearly identified, including the following information:

(a) the name of the evaluated ICT product;

(b) an enumeration of the ICT product's components that are part of the evaluation;

(c) the version number of the ICT product's components;

(d) identification of additional requirements to the operating environment of the certified ICT product;

(e) name and contact information of the holder of the EUCC certificate;

(f) where applicable, the patch management procedure included into the certificate;

(g) link to the website of the holder of the EUCC certificate where supplementary cybersecurity information for the certified ICT product in accordance with Article 55 of Regulation (EU) 2019/881 is provided.

6. The information included in this Section shall be as accurate as possible in order to ensure a complete and accurate representation of the ICT product that can be re-used in future evaluations.

7. The security policy section shall contain the description of the ICT product's security policy and the policies or rules that the evaluated ICT product shall enforce or comply with. It shall include a reference and a description of the following policies:

(a) the vulnerability handling policy of the holder of the certificate;

(b) the assurance continuity policy of the holder of the certificate.

8. Where applicable, the policy may include the conditions related to the use of a patch management procedure during the validity of the certificate.

9. The section for the assumptions and clarification of scope shall contain exhaustive information regarding the circumstances and objectives related to the intended use of the product as referred to in Article 6(1), point (c). The information shall include the following:

(a) assumptions on the ICT product's usage and deployment in the form of minimum requirements, such as proper installation and configuration and hardware requirements being satisfied;

(b) assumptions on the environment for the compliant operation of the ICT product;

10. The information listed in point 9 shall be as understandable as possible in order to let users of the certified ICT product make informed decisions about the risks associated with its use.

11. The architectural information section shall include a high-level description of the ICT product and its main components in accordance with Common Criteria's ADV_TDS subsystems design.

12. A complete listing of the ICT product supplementary cybersecurity information shall be provided in accordance with Article 55 of Regulation (EU) 2019/881. All relevant documentation shall be denoted by the version numbers.

13. The ICT product testing section shall include the following information:

    (a) the name and point of contact of the authority or body that issued the certificate including the responsible national cybersecurity certification authority;

    (b) the name of the ITSEF which performed the evaluation, when different from the certification body;

    (c) an identification of the used assurance components from the standards referred by Article 3;

    (d) the version of the state-of-the-art document and further security evaluation criteria used in the evaluation;

    (e) the complete and precise settings and configuration of the ICT product during the evaluation, including operational notes and observations if available;

    (f) any protection profile that has been used, including the following information:

        (1) the author of the protection profile;

        (2) the name and identifier of the protection profile;

        (3) the identifier of the protection profile's certificate;

        (4) the name and contact details of the certification body and of the ITSEF involved in the evaluation of the protection profile;

        (5) the assurance package(s) required for a product conforming to the protection profile.

14. The results of the evaluation and information regarding the certificate section shall include the following information:

    (a) confirmation of the attained assurance level as referred to in Article 4 of this Regulation and Article 52 in Regulation (EU) 2019/881;

    (b) assurance requirements from the standards referred by Article 3 that the ICT product or protection profile actually meets, including the AVA_VAN level;

    (c) detailed description of the assurance requirements, as well as the details of how the product meets each of them;

    (d) date of issuance and period of validity of the certificate;

    (e) unique identifier of the certificate.

15. The security target shall be included in the certification report or referenced and summarised in the certification report and provided with the certification report association with it for the purposes of publication.

16. The security target may be sanitised in accordance with Section III.2.

17. The mark or label associated to the EUCC may be inserted the certification report in accordance with the rules and procedures laid down Article 15.

18. The bibliography section shall include references to all documents used in the compilation of the certification report. That information shall include at least the following:

    (a) the security evaluation criteria, state-of-the-art documents and further relevant specifications used and their version;

    (b) the evaluation technical report;

    (c) the evaluation technical report for composite evaluation, where applicable;

    (d) technical reference documentation;

    (e) developer documentation used in the evaluation effort.

19. In order to guarantee the reproducibility of the evaluation, all documentation referred to has to be uniquely identified with the proper release date, and proper version number.

III.2 Sanitization of a security target for publication

1. The security target to be included in or referenced by the certification report pursuant to point 1 of Section III.1 may be sanitised by the removal or paraphrasing of proprietary technical information.

2. The resulting sanitised security target shall be a real representation of its complete original version. This means that the sanitised security target cannot omit information which is necessary to understand the security properties of the target of evaluation and the scope of the evaluation.

3. The content of the sanitised security target shall conform to the following minimum requirements:

    (a) its introduction shall not be sanitised as it includes no proprietary information in general;

    (b) the sanitised security target has to have a unique identifier that is distinct from its complete original version;

    (c) the target of evaluation description may be reduced as it may include proprietary and detailed information about the target of evaluation design which should not be published;

    (d) the target of evaluation security environment description (assumptions, threats, organisational security policies) shall not be reduced, in so far as that information is necessary to understand the scope of the evaluation;

    (e) the security objectives shall not be reduced as all information is to be made public to understand the intention of the security target and target of evaluation;

    (f) all security requirements shall be made public. Application notes may give information on how the functional requirements of the Common Criteria as referred to in Article 3 were used to understand the security target;

(g) the target of evaluation summary specification shall include all target of evaluation security functions but additional proprietary information may be sanitised;

(h) references to protection profiles applied to the target of evaluation shall be included;

(i) the rationale may be sanitised to remove proprietary information.

4. Even if the sanitised security target is not formally evaluated in accordance with the evaluation standards referred to in Article 3, the certification body shall ensure that it complies with the complete and evaluated security target, and reference both the complete and the sanitised security target in the certification report.

ANNEX IV: Scope and team composition for peer assessments

IV.1 Scope of the peer assessment

1. The following types of peer assessments are covered:

   (a) Type 1: when a certification body performs certification activities at the AVA_VAN.3 level;

   (b) Type 2: when a certification body performs certification activities related to a technical domain 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).

2. The peer-assessed certification body shall submit the list of certified ICT products that may be candidate to the review by the peer assessment team, in accordance with the following rules:

   (a) the candidate products shall cover the technical scope of the certification body authorisation, of which at least two different products evaluations at assurance level 'high' will be analysed through the peer assessment, and one protection profile if the certification body has issued certificate at assurance level 'high';

   (b) for a Type 2 peer assessment, the certification body shall submit at least one product per technical domain and per concerned ITSEF;

   (c) for a Type 3 peer assessment, at least one candidate product shall be evaluated in accordance with an applicable and relevant protection profiles.

IV.2 Peer assessment team

1. The assessment team shall consist of at least two experts each selected from a different certification body from different Member States that issues certificates at the assurance level 'high', and who both cover the relevant expertise in the standards as referred in Article 3 and state-of-the-art documents that are in scope of the peer assessment.

2. In the case of a delegation of certificate issuance or prior approval of certificates as referred to in Article 56(6) of Regulation (EU) 2019/881, an expert from the national cybersecurity certification authority related to the concerned certification body shall participate in the team of experts selected in accordance with paragraph 1 of this Section.

3. For a Type 2 peer assessment the team members shall be selected from certification bodies being authorised for the concerned technical domain.

4. Each member of the assessment team shall have at least two years of experience of carrying out certification activities in a certification body;

5. For a Type 2 or 3 peer assessment, each member of the assessment team shall have at least two years of experience of carrying out certification activities in that relevant technical domain or protection profile and proven expertise and participation in the authorisation of an ITSEF as specified in Article 9.

6. The national cybersecurity certification authority monitoring and supervising the peer-assessed certification body and at least one national cybersecurity certification authority whose certification body is not subject to the peer assessment shall

participate in the peer assessment as an observer. ENISA may also participate in the peer assessment as an observer.

7. The peer-assessed certification body is presented with the composition of the peer assessment team. In justified cases, it may challenge the composition of the peer assessment team and ask for its review.

ANNEX V: Content of an EUCC Certificate

Content of an EUCC certificate for the ICT product::

(a) a unique identifier established by the certification body issuing the certificate;

(b) information related to the certified ICT product and the holder of the certificate, including:

  (1) name of the ICT product and, where applicable, of the target of evaluation;

  (2) type of ICT product and, where applicable, of the target of evaluation;

  (3) version of the ICT product;

  (4) name, address and contact information of the holder of the certificate;

  (5) link to the website of the holder of the certificate containing the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881;

(c) information related to the evaluation and certification of the ICT product, including:

  (1) name, address and contact information of the certification body that issued the certificate;

  (2) where different from the certification body, name of the ITSEF which performed the evaluation;

  (3) name of the responsible national cybersecurity certification authority;

  (4) a reference to this Regulation;

  (5) a reference to the certification report associated with the certificate referred to in Annex III;

  (6) the applicable assurance level in accordance with Article 4;

  (7) a reference to the version of the standards used for the evaluation, referred to in Article 3 ;

  (8) identification of the assurance level or package specified in the standards referred to in Article 3 and in conformity with Annex VI, including the assurance components used and the AVA_VAN level covered;

  (9) where applicable, reference to one or more protection profiles with which the ICT product complies;

  (10) date of issuance;

  (11) period of validity of the certificate in accordance with Article 17;

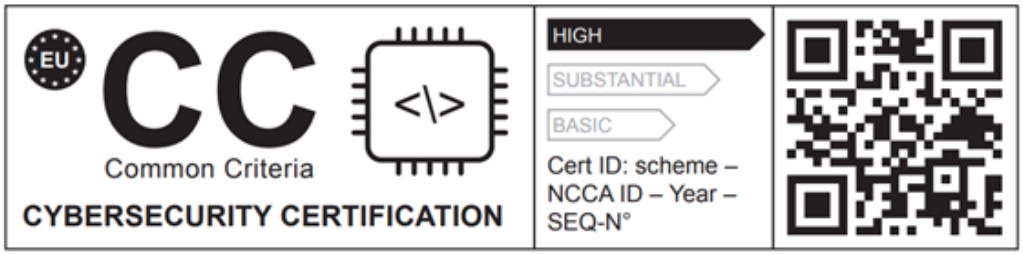
(d) the mark and label associated with the ICT product certification in accordance with Article 15.

ANNEX VI: Assurance package declaration

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

ANNEX VII: Mark and label

1. The form of mark and label:



2. If the mark and label are reduced or enlarged, the proportions given in the drawing above shall be respected.

3. Where physically present, the mark and label shall be at least 5 mm high.