Official Journal
of the European Union

EN
L series

2025/2462

9.12.2025

COMMISSION IMPLEMENTING REGULATION (EU) 2025/2462

of 8 December 2025

amending Implementing Regulation (EU) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art documents

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

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

Having regard to Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) ([1]), and in particular Article 49(7) thereof,

Whereas:

(1) Commission Implementing Regulation (EU) 2024/482 ([2]) specifies the roles, rules and obligations, as well as the structure of the European Common Criteria-based cybersecurity certification scheme (EUCC) in accordance with the European cybersecurity certification framework set out in Regulation (EU) 2019/881.

(2) The Common Evaluation Methodology accompanying the Common Criteria (CC), an international standard for information security evaluation, allows the evaluation of the security of ICT products for certification purposes. In that context, some ICT products may be built upon the same functional basis in order to offer similar security functionalities on different platforms or appliances, also referred to as a product series. However, the design, hardware, firmware or software may vary from one ICT product to another. It is for the certification body to decide on a case-by-case basis whether certification of a product series can be carried out. The conditions for product series certification could be further illustrated in supporting EUCC guidelines.

(3) In order to maintain the reliability of certified products, it is essential to define what constitutes a major and minor change to the target of evaluation or its environment, including its operational or development environments. Therefore, it is necessary to specify those notions considering existing and widely used technical specifications from the Senior Officials Group - Information Systems Security (SOG-IS) and the participants of the Arrangements on the Recognition of Common Criteria Certificates in the field of IT Security (CCRA).

(4) Minor changes are often characterised by their limited effect on the product assurance statement provided by the issued EUCC certificate. Thus, minor changes should be managed under maintenance procedures and do not require a re-evaluation of the security functionalities of the product. Examples of minor changes that should be addressed through maintenance include, but are not limited to, editorial changes, changes to the target of evaluation environment that do not modify the certified target of evaluation, and changes to the certified target of evaluation that do not affect the assurance evidences. Changes to the development environment may also be considered minor, provided they have no follow-on impact on existing assurance measures. They may however in some cases require partial evaluation of the relevant measures.

([1]) OJ L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

([2]) Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) (OJ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(5) A major change is any change to the certified target of evaluation or its environment that may adversely impact the assurance expressed in the EUCC certificate, hence it should require re-evaluation. Examples of major changes include, but are not limited to, changes to the set of claimed assurance requirements, except for the assurance requirements of the CC ALC_FLR family (Flaw remediation); changes to the confidentiality or integrity controls of the development environment where such modifications could affect the secure development or production of the target of evaluation or changes to the target of evaluation to resolve an exploitable vulnerability. Additionally, a collection of minor changes that collectively exerts a significant impact on the security may also be qualified as a major change. It is also important to recognise that while a bug fix may only affect a specific aspect of the target of evaluation, its unpredictability and potential impact on the assurance may render it a major change if it compromises the security assurances provided by the certification.

(6) Changes in the threat environment of an unchanged certified ICT product, could require a re-assessment. The possible outcomes of such re-assessment process should be clearly established, in particular its impact on the EUCC certificate. If a reassessment is successfully completed, the certification body should confirm the certificate or issue a new certificate with an extended expiry date. If a reassessment process is not successful, the certification body should withdraw the certificate and possibly issue a new certificate with a different scope. Such provisions should apply *mutatis mutandis* to the reassessment of protection profiles.

(7) Annex I to Implementing Regulation (EU) 2024/482 lists applicable state-of-the-art documents for the evaluation of ICT products and protection profiles. Those state-of-the-art documents should be updated to reflect the latest developments, such as those related to technological developments, the cyber threat landscape, industry practices, or international standards. Such an update is opportune for the state-of-the-art documents relating to minimum site security requirements, application of attack potentials to smartcards, application of attack potentials to hardware devices with security boxes, application of common criteria to integrated circuits and composite product evaluation for smartcards and similar devices. Additionally, state-of-the-art documents relating to composite product evaluation and certification using the latest version of the Common Criteria standards, reuse of evaluation results of site audits and clarifications regarding the interpretation of protection profiles relating to qualified electronic signature creation devices, tachographs and hardware security modules are not included. In order to ensure a uniform evaluation of ICT products under the EUCC, Annex I should be amended to include those updated and new state-of-the-art documents following their endorsement by the European Cybersecurity Certification Group (ECCG).

(8) Additionally, the state-of-the-art document 'ADV_SPM.1 interpretation for CC:2022 transition' should be added to the scheme to ensure that certification processes relying on specific protection profiles can continue using formal modelling (ADV_SPM.1) until the corresponding protection profiles are updated, for instance with the addition of a CC:2022 conformant multi-assurance protection profile configuration that supports ADV_SPM.1. In order to provide sufficient time for the market to transition towards the updated Common Criteria standards, specific transition rules need to be foreseen for the protection profiles Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014, Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, or Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020. To avoid any market disruptions, it is appropriate to establish that the state-of-the-art document on ADV_SPM.1 interpretation for CC:2022 transition is applicable to certification processes that have been initiated before the adoption of this Regulation. The application of this document should be, however, strictly limited to what is necessary, considering the time needed to finalise the update of the corresponding protection profiles. More precisely, for certification processes using protection profiles Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014, or Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, the state-of-the-art document should apply to those processes that have been initiated before 1 October 2026. For certification processes using protection profile Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020, the state-of-the-art document should only apply to those processes initiated before the date of entry into force of this Regulation, in view that a new version of the Java Card System – Open Configuration protection profile is already available.

(9) A change in the state-of-the-art documents during a certification process could disrupt the evaluation of the product and delay the issuance of the certificate. Therefore, appropriate transition rules are necessary for new or updated state-of-the-art documents, to enable vendors, ITSEFs, certification bodies and other stakeholders to make necessary adjustments. Applicable updated and new state-of-the-art documents should concern applications for certification, including applications for reassessment and re-evaluation, while it should be possible for ongoing certification processes to keep using earlier versions of the state-of-the-art documents.

(10) Annex II and Annex III to Implementing Regulation (EU) 2024/482 list respectively the protection profiles certified at AVA_VAN level 4 or 5 and the recommended protection profiles. Several references are incomplete or obsolete, due to an update of the protection profiles. Those references should be completed and, in addition, new references should be included to ensure a more comprehensive coverage of secure integrated circuits, smartcards and related devices and trusted computing.

(11) It is necessary to make amendments to Article 19 of Implementing Regulation (EU) 2024/482 to clarify that Annex IV applies, with the necessary changes, to the review of EUCC certificates for protection profiles.

(12) In view that the security target is a key element to understand the scope of a certification process, it is also necessary for ENISA to publish the security target corresponding to each EUCC certificate on its website.

(13) Furthermore, certification bodies should provide ENISA with an English version of the security target and the certification report to enable the agency to make that information available in English on the corresponding website, pursuant to Article 42(2) of Implementing Regulation (EU) 2024/482. For that reason, applicants for certification should provide certification bodies with an English version of the security target, whenever requested.

(14) It is not necessary for the reference to the certification body name to appear in the unique identification of the certificate as the identification number of the certification body is sufficient to identify this body in a unique manner. The month of issuance does not need to appear either as the counting of the certificates is done on a yearly basis. Therefore, that requirement should be deleted for simplification purposes. Since the year of issuance of the certificate corresponds to the issuance of the first certificate, that same date should appear in the unique identification on certificates issued after a review, to ensure traceability.

(15) Implementing Regulation (EU) 2024/482 should therefore be amended accordingly.

(16) The measures provided for in this Regulation are in accordance with the opinion of the Committee established by Article 66 of Regulation (EU) 2019/881,

HAS ADOPTED THIS REGULATION:

Article 1

Implementing Regulation (EU) 2024/482 is amended as follows:

(1) in Article 2, the following points (16), (17) and (18) are added:

'(16) "product series" means a set of ICT products by an applicant, built upon the same functional basis in order to address the same security needs, having a design, hardware, firmware or software which may vary from an ICT product to another;

(17) "minor change" means any change in the certified target of evaluation or its environment that does not adversely impact the assurance expressed in the EUCC certificate;

(18) "major change" means any change in the certified target of evaluation or its environment that may adversely impact the assurance expressed in the EUCC certificate.';

(2) in Article 5, the following paragraph 3 is added:

'3. A certification body may allow the certification of a product series.';

(3) in Article 9, paragraph 2, point (a) is replaced by the following:

'(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, including an English version of the security target;';

(4) in Article 11, paragraph 3, point (b) is replaced by the following:

'(b) the unique identification of the certificate, consisting of:

(1) the name of the scheme;

(2) the identification number, in accordance with Article 3 of Implementing Regulation (EU) 2024/3143, of the certification body that has issued the certificate;

(3) year of issuance of the initial certificate;

(4) identification number assigned by the certification body that has issued the certificate.';

(5) in Article 19, paragraph 1 is replaced by the following:

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

(6) Article 42 is amended as follows:

(a) in paragraph 1, the following point (i) is added:

'(i) the security target corresponding to each EUCC certificate;';

(b) paragraph 2 is replaced by the following:

'2. The information referred to in paragraph 1 shall be made available at least in English. For that purpose, certification bodies shall provide ENISA with the original language versions of the certification reports and security targets, and in addition they shall also provide the English version of such documents without undue delay.';

(7) in Article 48, paragraph 4 is replaced by the following:

'4. Unless specified otherwise in Annex I or II, state-of-the-art documents shall apply to certification processes, including reassessment and re-evaluation, initiated from the date of application of the amending act by which the state-of-the-art documents have been incorporated in Annex I or II.';

(8) Annex I is replaced by the text in Annex I to this Regulation;

(9) Annex II is replaced by the text in Annex II to this Regulation;

(10) Annex III is replaced by the text in Annex III to this Regulation;

(11) Annex IV is amended in accordance with Annex IV to this Regulation;

(12) Annex V is amended in accordance with Annex V to this Regulation;

(13) Annex IX is replaced by the text in Annex VI to this Regulation.

Article 2

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

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

Done at Brussels, 8 December 2025.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX I

'ANNEX I

State-of-the-art documents supporting technical domains and other state-of-the-art documents

1. State-of-the-art documents supporting technical domains at AVA_VAN level 4 or 5:
   (a) the following documents related to the harmonised evaluation of technical domain "smart cards and similar devices":
      (1) "Minimum ITSEF requirements for security evaluations of smart cards and similar devices", version 1.1;
      (2) "Minimum Site Security Requirements", version 2;
      (3) "Reusing evaluation results of site audits (STAR)", version 1;
      (4) "Application of Common Criteria to integrated circuits", version 2;
      (5) "Security Architecture requirements (ADV_ARC) for smart cards and similar devices", version 1.1;
      (6) "Certification of 'open' smart card products", version 1.1;
      (7) "Composite product evaluation for smart cards and similar devices for CC3.1", version 2;
      (8) "Composite product evaluation and certification for CC:2022", version 1;
      (9) "Application of Attack Potential to Smartcards and Similar Devices", version 2;
      (10) "Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices", version 1;
      (11) "ADV_SPM.1 interpretation for CC:2022 transition", version 1.1, applicable for certification processes using protection profiles as follows:
         (a) protection profiles Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014, or Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, initiated before 1 October 2026;
         (b) protection profile Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020, initiated before 29 December 2025.
   (b) the following documents related to the harmonised evaluation of technical domain "hardware devices with security boxes":
      (1) "Minimum ITSEF requirements for security evaluations of hardware devices with security boxes", version 1.1;
      (2) "Minimum Site Security Requirements", version 2;
      (3) "Reusing evaluation results of site audits (STAR)", version 1;
      (4) "Application of Attack Potential to hardware devices with security boxes", version 2;
      (5) "Hardware assessment in EN 419221-5 (HSM PP)", version 1;
      (6) "JIL Tachograph MS PP Clarification", version 1.

2. State-of-the-art documents related to the harmonised accreditation of conformity assessment bodies:
   (a) "Accreditation of ITSEFs for the EUCC", version 1.1 for accreditations issued before 8 July 2025;
   (b) "Accreditation of ITSEFs for the EUCC", version 1.6c, for accreditations that are newly issued or reviewed after 8 July 2025;
   (c) "Accreditation of CBs for the EUCC", version 1.6b.'

ANNEX II

'ANNEX II

Protection profiles certified at AVA_VAN level 4 or 5

1. For remote qualified signature and seal creation devices:

   (a) EN 419241-2:2019 – Trustworthy Systems Supporting Server Signing – Part 2: Protection Profile for QSCD for Server Signing (v0.16), ANSSI-CC-PP-2018/02-M01;

   (b) EN 419221-5:2018 – Protection profiles for Trust Service Provider Cryptographic modules – Part 5: Cryptographic Module for Trust Services (v0.15), ANSSI-CC-PP-2016/05-M01.

2. Protection profiles that have been adopted as state-of-the-art documents:

   [BLANK].'

ANNEX III

'ANNEX III

Recommended protection profiles

Protection profiles used in certification of ICT products including products in the technical domains:

1. Smartcards and similar devices:

   (a) passport:

      (1) PP Machine Readable Travel Document with 'ICAO Application' Basic Access Control (v1.10), BSI-CC-PP-0055-2009;

      (2) PP Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP) (v1), BSI-CC-PP-0068-V2-2011-MA-01;

      (3) PP Machine Readable Travel Document with 'ICAO Application' Extended Access Control with PACE (v1.3), BSI-CC-PP-0056-V2-2012-MA-02;

   (b) Secure Signature Creation Devices (SSCD):

      (1) EN 419211-2:2013 – Protection profiles for secure signature creation device – Part 2: Device with key generation (v1.03), BSI-CC-PP-0059-2009-MA-02;

      (2) EN 419211-3:2013 – Protection profiles for secure signature creation device – Part 3: Device with key import (v1.0.2), BSI-CC-PP-0075-2012-MA-01;

      (3) EN 419211-4:2013 – Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application (v1.0.1), BSI-CC-PP-0071-2012-MA-01;

      (4) EN 419211-5:2013 – Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application (v1.0.1), BSI-CC-PP-0072-2012-MA-01;

      (5) EN 419211-6:2014 – Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted channel to signature creation application (v1.0.4), BSI-CC-PP-0076-2013-MA-01;

   (c) tachograph: Digital Tachograph – Tachograph Card (TC PP) (v1.0), BSI-CC-PP-0091-2017;

   (d) secure IC, Java Card platform and eUICC:

      (1) Universal SIM Java Card Platform Protection Profile Basic and SCWS Configurations (v2.0.2), ANSSI-CC-PP-2010/04 (Basic), ANSSI-CC-PP-2010/05 (Basic and SCWS);

      (2) Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014;

      (3) Embedded UICC (eUICC) for Machine-to-Machine Devices (v1.1), BSI-CC-PP-0089-2015;

      (4) Cryptographic Service Provider – CSP (v0.9.8), BSI-CC-PP-0104-2019;

      (5) Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au) Version 0.9.5, BSI-CC-PP-0107-2019;

      (6) Configuration Cryptographic Service Provider – Time Stamp Service, Audit and Clustering (PPC-CSP-TS-Au-Cl) Version 0.9.4, BSI-CC-PP-0108-2019;

      (7) Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020;

      (8) Secure Element Protection Profile – GPC_SPE_174 (v1.0), CCN-CC-PP-5-2021;

      (9) Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile (v1.8), BSI-CC-PP-0117-V2-2023;

      (10) Java Card System – Open Configuration (v3.2), BSI-CC-PP-0099-V3-2024;

      (11) Embedded UICC for Consumer Devices Protection Profile (v2.1), BSI-CC-PP-0100-V2-2025;

   (e) Trusted Platform Module: Protection Profile PC Client Specific Trusted Platform Module Specification Family 2.0; Level 0; Revision 1.59 (v1.3), ANSSI-CC-PP-2021/02.

2. Hardware Devices with Security Boxes:
   (a) points of (payment) interaction and payment terminals (POI):
      (1) Point of Interaction 'POI-CHIP-ONLY' (v4.0), ANSSI-CC-PP-2015/01;
      (2) Point of Interaction 'POI-CHIP-ONLY and Open Protocol Package' (v4.0), ANSSI-CC-PP-2015/02;
      (3) Point of Interaction 'POI-COMPREHENSIVE' (v4.0), ANSSI-CC-PP-2015/03;
      (4) Point of Interaction 'POI-COMPREHENSIVE and Open Protocol Package' (v4.0), ANSSI-CC-PP-2015/04;
      (5) Point of Interaction 'POI-PED-ONLY' (v4.0), ANSSI-CC-PP-2015/05;
      (6) Point of Interaction 'POI-PED-ONLY and Open Protocol Package' (v4.0), ANSSI-CC-PP-2015/06;
   (b) Hardware Security Module:
      (1) Cryptographic Module for CSP Signing Operations with Backup – PP CMCSOB 14167-2 (v0.35), ANSSI-CC-PP-2015/08;
      (2) Cryptographic Module for CSP Key Generation Services – PP CMCKG 14167-3 (v0.20), ANSSI-CC-PP-2015/09;
      (3) Cryptographic Module for CSP Signing Operations without Backup – PP CMCSO 14167-4 (v0.32), ANSSI-CC-PP-2015/10;
   (c) tachograph:
      (1) Digital Tachograph – Motion Sensor (MS PP) (v1.0), BSI-CC-PP-0093-2017;
      (2) Digital Tachograph – Vehicle Unit (VU PP) (v1.15), BSI-CC-PP-0094-V2-2021;
      (3) Digital Tachograph – External GNSS Facility (EGF PP) (v1.10), BSI-CC-PP-0092-V2-2021.
3. Others: Trusted Execution Environment Protection Profile – GPD_SPE_021 (v1.3), ANSSI-CC-PP-2014/01-M02.'

ANNEX IV

Annex IV to Implementing Regulation (EU) 2024/482 is amended as follows:

1. in point IV.2, point 4 is replaced by the following:

   '4. The certification body shall review the updated evaluation technical report and establish a re-assessment report. The status of the initial certificate shall then be modified in accordance with Article 13 or Article 19. If the re-assessment process is successful, Article 13 paragraph 2 points (a) or (c) applies in the case of the certification of a product and Article 19 paragraph 2 point (a) or (c) applies in the case of the certification of a protection profile. If the re-assessment process is not successful, Article 13 paragraph 2 point (b) or (d) applies in the case of the certification of a product and Article 19 paragraph 2 point (b) or (d) applies in the case of the certification of a protection profile.';

2. point IV.3 is amended as follows:

   (a) Title IV.3 is replaced by the following:

   'IV.3 **Changes to a certified ICT product – Maintenance and re-evaluation**';

   (b) points 4 and 5 are replaced by the following:

   '4. Following the examination, the certification body determines the scale of a change as minor or major in correspondence to its impact on the assurance expressed in the EUCC certificate.

   5. Where the changes have been confirmed by the certification body to be minor, no new certificate shall be issued for the modified ICT product in accordance with Article 13 paragraph 2 point (a) or Article 19 paragraph 2 point (a) and a maintenance report to the initial certification report shall be established.';

   (c) the following point 5a is inserted:

   '5.a In case of any changes to the assurance measures in the development environment, including the addition of assurance requirements from the CC ALC_FLR family (Flaw remediation), the certification body may request the ITSEF to perform a subset evaluation of the affected assurance measures. The ITSEF shall issue a partial evaluation technical report, based on which the certification body confirms the changes to be either minor or major. Where the changes have been confirmed by the certification body to be minor, Annex IV.3 point 5 shall apply. Where the changes have been confirmed by to the certification body to be major, Annex IV.3 point 7 shall apply.'.

ANNEX V

Point V.1 of Annex V to Implementing Regulation (EU) 2024/482 is replaced by the following:

'V.1 **Certification report**

1. Based on the evaluation technical reports provided by the ITSEF, the certification body establishes a certification report to be published together with the corresponding EUCC certificate and security target.

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

3. The certification report shall contain at least the following information:
   (a) executive summary;
   (b) identification of the ICT product;
   (c) contact information related to the evaluation of the ICT product;
   (d) security policies;
   (e) assumptions and clarification of scope;
   (f) architectural information;
   (g) supplementary cybersecurity information, if applicable;
   (h) ICT product evaluation summary and evaluated configuration;
   (i) results of the evaluation and information regarding the certificate;
   (j) comments and recommendations if applicable;
   (k) annexes, if applicable;
   (l) reference to the security target of the ICT product submitted to certification;
   (m) when available, the mark or label associated to the scheme;
   (n) glossary, if applicable;
   (o) bibliography.

4. The executive summary referred to in paragraph 3, point (a) shall be a brief summary of the entire certification report. It shall provide a clear and concise overview of the evaluation results and shall include the following information:
   (a) name of the evaluated ICT product;
   (b) name of the ITSEF which performed the evaluation;
   (c) completion date of evaluation;
   (d) date of issuance of the certificate;
   (e) where applicable, date of issuance of the initial certificate;
   (f) validity period;
   (g) unique identification of the certificate as described in Article 11;
   (h) brief description of the certification report results, including:
      (i) the version and if applicable release of the Common Criteria applied to the evaluation;
      (ii) the Common Criteria assurance package or list of security assurance components, the AVA_VAN level applied during the evaluation and the corresponding assurance level as set out in Article 52 of Regulation (EU) 2019/881 to which the EUCC certificate refers to;
      (iii) where applicable, the Protection Profile(s) to which the ICT product is claiming compliance to;
      (iv) reference to the security policy of the evaluated ICT product;
      (v) disclaimer(s), if applicable.

5. The identification referred to in paragraph 3, point (b) shall clearly identify the evaluated ICT product, including the following information:

   (a) the unique identification of the evaluated ICT product;

   (b) enumeration of the ICT product's components that are part of the evaluation with version number of each component;

   (c) reference to additional requirements to the operational environment of the certified ICT product.

6. The contact information referred to in paragraph 3, point (c) shall include at least the following information:

   (a) name of the developer;

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

   (c) name of the certification body that issued the certificate;

   (d) responsible national cybersecurity certification authority;

   (e) name of the ITSEF which performed the evaluation, and, where applicable, the list of subcontractors.

7. The security policy referred to in paragraph 3, point (d), shall contain the description of the ICT product's security policy as a collection of security services and the policies or rules that the evaluated ICT product shall enforce or comply with. It shall also include the following information:

   (a) a description of the vulnerability management and vulnerability disclosure procedures of the certificate holder, to be completed solely with information that can be made publicly available;

   (b) the assurance continuity policy of the holder of the certificate, including, where applicable, the description of the certificate holder's lifecycle management or production processes in accordance with Section IV.1 of Annex IV;

   (c) where applicable, the presence of patch management procedure and the outcome of its assessment in accordance with Section IV.4 of Annex IV.

8. The assumptions and clarification of scope referred to in paragraph 3, point (e), shall contain information regarding the circumstances and objectives related to the intended use of the product as referred to in Article 7(1), point (c) and 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;

   (c) description of any threats to the ICT product that are not countered by the evaluated security functions of the product according to the intended use, if deemed relevant for a potential ICT product user.

   The information referred to in the first subparagraph shall be as clear and understandable as possible to enable potential users of the certified ICT product to make informed decisions about the risks associated with its use.

9. The architectural information referred to in paragraph 3, point (f), shall include a high-level description of the ICT product and its main components, based on the deliverables defined in the Common Criteria assurance family: Development – TOE Design (ADV_TDS).

10. The supplementary cybersecurity information referred to in paragraph 3, point (g) shall include the link to the website of the holder of the EUCC certificate referred to in Article 55 of Regulation (EU) 2019/881.

11. The ICT product evaluation and configuration referred to in paragraph 3, point (h), shall describe both the developer and evaluator testing effort, outlining the testing approach, configuration and depth. It shall include at least the following information:

    (a) an identification of the used assurance components from the standards referred in Article 3;

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

    (c) the settings and configuration of the TOE used for the testing and vulnerability analysis;

    (d) any protection profile that has been used, including the following information: the protection profile name, version, date and certificate.

12. The results of the evaluation and information regarding the certificate referred to in paragraph 3, point (i) shall include information on the attained assurance level as referred to in Article 4 of this Regulation and Article 52 of Regulation (EU) 2019/881.

13. The comments and recommendations referred to in paragraph 3, point (j), are used to impart additional information about the evaluation results. Those comments and recommendations may take the form of shortcomings of the ICT product discovered during the evaluation or mentions of features which are particularly useful.

14. The Annexes referred to in paragraph 3, point (k), are used to outline any additional information that may be useful to the audience of the report but does not logically fit within the prescribed sections of the report, including in cases of a complete description of security policy.

15. The security target referred to in paragraph 3, point (l), shall reference the evaluated security target. The evaluated security target shall be provided with the certification report for the purposes of publication on the website referred to in Article 50(1) of Regulation (EU) 2019/881. Where sanitisation of the evaluated security target is necessary prior to publication, it shall be done in accordance with point V.2 of Annex V to this Regulation.

16. The marks or labels associated to the EUCC scheme referred to in paragraph 3, point (m), shall be inserted in the certification report in accordance with the rules and procedures laid down in Article 11.

17. The Glossary referred to in paragraph 3, point (n), is used to increase the readability of the report by providing definitions of acronyms or terms of which the meanings may not be readily apparent.

18. The bibliography referred to in paragraph 3, point (o), 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;

    (b) the evaluation technical report;

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

    (d) technical reference documentation;

    (e) developer security guidance;

    (f) developer configuration list.

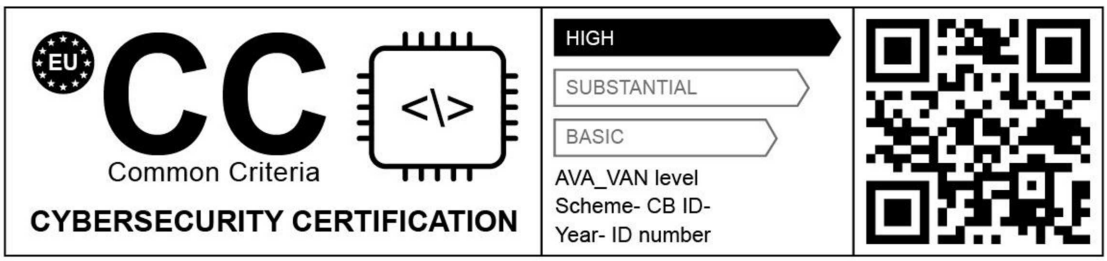
    In order to guarantee the reproducibility of the evaluation, all documentation referred to has to be uniquely identified with the proper release date and proper version number.'.

ANNEX VI

'*ANNEX IX*

Mark and label

1. The form of mark and label:



2. If the mark and label are reduced or enlarged, the proportions given in point 1 shall be respected.

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