Official Journal
of the European Union

EN
L series

2024/3144

19.12.2024

COMMISSION IMPLEMENTING REGULATION (EU) 2024/3144

of 18 December 2024

amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation

(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) Implementing Regulation (EU) 2024/482 is based on established international standards that are the Common Criteria and the Common Evaluation Methodology maintained by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Implementing Regulation (EU) 2024/482 makes reference to ISO/IEC standards, but it does not specify the applicable version of those standards. It should therefore be specified which version of the standards applies for certificates issued under the EUCC.

(3) The governmental organisations that contributed to the development of the Common Criteria and the Common Evaluation Methodology through the Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security (CCRA) are joint holders, together with the ISO/IEC of the copyrights to them. Those governmental organisations retain the right to use them. In view of the importance of those documents originating from the CCRA, they should also be a basis for certification under the EUCC.

(4) The Common Criteria and the Common Evaluation Methodology standards are subject to interpretations done by the CCRA that facilitate their implementation and that may be considered by Information Technology Security Evaluation Facilities (ITSEFs) and certification bodies.

(5) International standards related to the Common Criteria might be subject to updates. To ensure an orderly and timely transition, it is appropriate to define transition rules to give vendors, ITSEFs and certification bodies, and other relevant actors enough time for the necessary adjustments. Such transition rules should align to the appropriate extent with global practices, such as those set out by the CCRA.

([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).

(6) Implementing Regulation (EU) 2024/482 does not specify until when an ICT product certification might be based on the previous versions of the Common Criteria and the Common Evaluation Methodology standards. Technical domains and protection profiles listed in Annexes I, II and III to that Implementing Regulation are based on previous versions of standards ISO/IEC 15408 and 18045. Implementing Regulation (EU) 2024/482 should therefore specify under what circumstances the previous version of the Common Criteria and the Common Evaluation Methodology still applies and how the transition to the latest version of the international standards will operate.

(7) During the transition period, it should be a priority for relevant stakeholders to update the relevant technical domains and protection profiles. Implementing Regulation (EU) 2024/482 should provide that security targets based on a previous version of the standards would be accepted up to 31 December 2027 in line with the transition policy adopted by the CCRA. However, it is to be noted that the CCRA transition policy covers initial evaluations of products and protection profiles starting no later than 30 June 2024, date at which the EUCC was not yet applicable. Furthermore, in accordance with the CCRA transition policy, Implementing Regulation (EU) 2024/482 should provide that security targets conformant to that Implementing Regulation claiming conformance to protection profiles based on a previous version of the standards would be accepted up to 31 December 2027. Furthermore, where a new certificate is issued under Implementing Regulation (EU) 2024/482 in the context of a review process of a national certificate that starts within two years from the initial certificate, it should be possible to use a previous version of the standards. This would not be relevant for a review process that does not require the issuance of a new certificate under Implementing Regulation (EU) 2024/482 and where the certificate remains valid.

(8) With a view to ensuring an orderly transition to the latest version of the standards, Implementing Regulation (EU) 2024/482 should provide for specific transition rules and continue to allow for the issuance of certificates under that Implementing Regulation claiming conformance to protection profiles that are based on previous versions of the standards published by the CCRA where the use of such protection profiles is required under Union legislation. This is the case for Commission Implementing Regulation (EU) 2016/799 ([3]) as well as Regulation (EU) No 910/2014 of the European Parliament and of the Council ([4]) and Commission Implementing Decision (EU) 2016/650 ([5]).

(9) Annex I to Implementing Regulation (EU) 2024/482 lists applicable state-of-the-art documents for the evaluation of ICT products and protection profiles. However, it does not specify the version of the documents. It should therefore be specified which version of the documents applies for certificates issued under the EUCC. Those versions build on documents endorsed by the European Cybersecurity Certification Group (ECCG), while having undergone further review for their inclusion in the EUCC. Furthermore, Annex I should be amended to include updated and new state-of-the-art documents following their endorsement by the ECCG, thus ensuring a uniform accreditation of conformity assessment bodies under the EUCC. The accreditation requirements related to the accreditation of ITSEFs should be updated to clarify the application of the criteria of independence and impartiality, and a new state-of-the-art document should be established for the accreditation of certification bodies.

(10) State-of-the-art documents might be added to the EUCC or might be subject to updates in the context of its maintenance activities. For new or updated state-of-the-art documents, appropriate transition rules might need to be laid down to enable vendors, ITSEFs, certification bodies and other stakeholders to make necessary adjustments. For the update of the state-of-the-art document related to the accreditation of ITSEFs, the updated document should apply to accreditations issued before 8 July 2025 only when they are reviewed, such as in the context of an assessment or re-assessment procedure. Furthermore, the updated document should apply to all accreditations for ITSEFs issued after 8 July 2025.

([3]) Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) No 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components (OJ L 139, 26.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

([4]) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([5]) Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ L 109, 26.4.2016, p. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).

(11) Further corrections to Articles 5, 8, 16, 29 and 44 and Annex IV of Implementing Regulation (EU) 2024/482 contribute to ensuring a uniform wording and clear legal interpretation.

(12) The rules for notifications of the conformity assessment bodies should be established horizontally for all schemes under the European cybersecurity certification framework. Commission Implementing Regulation (EU) 2024/3143 ([6]) covers such notification rules. Therefore, Articles 23 and 24 of Implementing Regulation (EU) 2024/482 should be deleted from the date Implementing Regulation (EU) 2024/3143 becomes applicable.

(13) Implementing Regulation (EU) 2024/482 should therefore be amended and corrected accordingly.

(14) 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, points (1) and (2) are replaced by the following:

'(1) "Common Criteria" means the Common Criteria for Information Technology Security Evaluation, as set out in standards ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022 or ISO/IEC 15408-5:2022, or set out in Common Criteria for Information Technology Security Evaluation, version CC:2022, Parts 1 through 5, published by the participants of the Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security;

(2) "Common Evaluation Methodology" means the Common Methodology for Information Technology Security Evaluation, as set out in standard ISO/IEC 18045:2022, or the Common Methodology for Information Technology Security Evaluation, version CEM:2022, published by the participants of the Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security;';

(2) Article 3 is replaced by the following:

'*Article 3*

Evaluation standards

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

(a) the Common Criteria;

(b) the Common Evaluation Methodology.

2. Until 31 December 2027, a certificate may be issued under the EUCC scheme applying either of the following standards:

(a) ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 or ISO/IEC 15408-3:2008;

(b) Common Criteria for Information Technology Security Evaluation, version 3.1, revision 5, published by the participants of the Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security;

([6]) Commission Implementing Regulation (EU) 2024/3143 of 18 December 2024 establishing the circumstances, formats and procedures for notifications pursuant to Article 61(5) of Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (OJ L, 2024/3143, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

(c) ISO/IEC 18045:2008;

(d) Common Methodology for Information Technology Security Evaluation, revision 5, version 3.1, published by the participants of the Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security.

3. Until 31 December 2027, a certificate applying the standards referred to in paragraph 1 may be issued under the EUCC scheme claiming conformance to a protection profile that has applied the standards listed in paragraph 2.

4. A certificate applying the standards referred to in paragraph 1 may also be issued under the EUCC scheme claiming conformance to a protection profile that has applied either of the following standards, provided that the use of such protection profile is required under Commission Implementing Regulation (EU) 2016/799 (*), Regulation (EU) No 910/2014 of the European Parliament and of the Council (**) or Commission Implementing Decision (EU) 2016/650 (***):

(a) Common Criteria for Information Technology Security Evaluation, version 3.1, revision 1 to 4, published by the participants of the Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security;

(b) Common Methodology for Information Technology Security Evaluation, version 3.1., revision 1 to 4, published by the participants of the Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security.

_____

(*) Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) No 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components (OJ L 139, 26.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

(**) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(***) Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ L 109, 26.4.2016, p. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).';

(3) in Chapter IV the following Article 20a is inserted:

'*Article 20a*

Specification of requirements for accreditation of conformity assessment bodies

The accreditation of conformity assessment bodies shall take into account the specification of requirements for accreditation of certification bodies and ITSEFs as laid down in the applicable state-of-the-art documents listed in point 2 of Annex I.';

(4) Articles 23 and 24 are deleted;

(5) in Article 48, the following paragraph 4 is added:

'4. Unless specified otherwise in Annex I or II, state-of-the-art documents shall apply from the date of application of the amending act by which they have been incorporated in Annex I or II.';

(6) in Article 49, the following paragraph 4 is added:

'4. When conducting the review referred to in paragraph 3 within two years of the issuance of initial certificate and where such a review leads to the issuance of a new certificate in accordance with this Regulation, the standards listed in Article 3(2) may be applied. The date of issuance of the initial certificate shall be understood as the date of issuance of the last certificate for a ICT product or protection profile on which the current certification is based on.';

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

(8) Annex IV is amended in accordance with Annex II to this Regulation.

Article 2

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

(1) in Article 5(1), point (b) is replaced by the following:

'(b) claiming conformance to a certified protection profile as part of the ICT process, where the ICT product falls in the ICT product category covered by that protection profile.';

(2) Article 8 is corrected as follows:

(a) the title is replaced by the following:

'Information necessary for certification and evaluation';

(b) paragraph 1 is replaced by the following:

'1. An applicant for certification under EUCC shall provide or otherwise make available to the certification body and the ITSEF all information necessary for the certification and evaluation activities.';

(3) Article 16 is replaced by the following:

'*Article 16*

Information necessary for certification and evaluation of protection profiles

An applicant for certification of a protection profile shall provide or otherwise make available to the certification body and the ITSEF all information necessary for the certification and evaluation activities in a complete and correct form. Article 8(2), (3), (4) and (7) shall apply *mutatis mutandis*.';

(4) in Article 17, paragraph 1 is deleted;

(5) in Article 29, paragraph 2 is replaced by the following:

'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 or Article 20.'.

Article 3

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

Article 1(4) shall apply from 8 January 2025.

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

Done at Brussels, 18 December 2024.

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 1.1;
      (3) "Application of Common Criteria to integrated circuits", version 1.1;
      (4) "Security Architecture requirements (ADV_ARC) for smart cards and similar devices", version 1.1;
      (5) "Certification of 'open' smart card products", version 1.1;
      (6) "Composite product evaluation for smart cards and similar devices", version 1.1;
      (7) "Application of Attack Potential to Smartcards and Similar Devices", version 1.2;
   (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 1.1;
      (3) "Application of Attack Potential to hardware devices with security boxes", version 1.2.

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

In Annex IV to Implementing Regulation (EU) 2024/482, Section IV.3, points 5 and 6 are replaced by the following:

‘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 and a maintenance report to the initial certification report shall be established.

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

(a) introduction;

(b) description of changes;

(c) affected developer evidence.

6. The maintenance report referred to in point 5 shall be provided to ENISA for publication on its cybersecurity certification website.’.