Journal officiel
de l'Union européenne

FR
Série L

2024/3144

19.12.2024

# RÈGLEMENT D'EXÉCUTION (UE) 2024/3144 DE LA COMMISSION

**du 18 décembre 2024**

**modifiant le règlement d'exécution (UE) 2024/482 en ce qui concerne les normes internationales applicables et rectifiant ledit règlement d'exécution**

**(Texte présentant de l'intérêt pour l'EEE)**

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) ([1]), et notamment son article 49, paragraphe 7,

considérant ce qui suit:

(1) Le règlement d'exécution (UE) 2024/482 de la Commission ([2]) précise les rôles, les règles et les obligations, ainsi que la structure du schéma européen de certification de cybersécurité (EUCC) fondé sur des critères communs, conformément au cadre européen de certification de cybersécurité défini dans le règlement (UE) 2019/881.

(2) Le règlement d'exécution (UE) 2024/482 est fondé sur des normes internationales établies, à savoir les critères communs et la méthode d'évaluation commune définis par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI). Le règlement d'exécution (UE) 2024/482 fait référence aux normes ISO/CEI mais il ne précise pas la version applicable de ces normes. Il convient donc de préciser quelle est la version des normes qui s'applique aux certificats délivrés au titre du schéma européen de certification de cybersécurité fondé sur des critères communs (EUCC).

(3) Les organisations gouvernementales qui ont contribué à l'élaboration des critères communs et de la méthode d'évaluation commune dans le cadre de l'accord de reconnaissance des certificats «Critères Communs dans le domaine de la sécurité informatique (CCRA)» sont cotitulaires, avec l'ISO et la CEI, des droits d'auteur qui y sont associés. Ces organisations gouvernementales conservent le droit de les utiliser. Compte tenu de leur importance, les documents émanant du CCRA devraient également servir de base à la certification au titre du schéma EUCC.

(4) Les normes relatives aux critères communs et à la méthode d'évaluation commune font l'objet d'interprétations de la part du CCRA qui facilitent la mise en œuvre de ces normes et qui peuvent être prises en compte par les centres d'évaluation de la sécurité des technologies de l'information (CESTI) et les organismes de certification.

(5) Les normes internationales relatives aux critères communs sont susceptibles de faire l'objet de mises à jour. Il convient, pour garantir une transition rapide et ordonnée, de définir des règles transitoires afin d'accorder suffisamment de temps aux vendeurs, aux CESTI, aux organismes de certification et aux autres acteurs concernés pour procéder aux adaptations nécessaires. Ces règles transitoires devraient être alignées, dans une mesure appropriée, sur les pratiques mondiales, telles que celles établies par le CCRA.

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

([2]) Règlement d'exécution (UE) 2024/482 de la Commission du 31 janvier 2024 portant modalités d'application du règlement (UE) 2019/881 du Parlement européen et du Conseil en ce qui concerne l'adoption du schéma européen de certification de cybersécurité fondé sur des critères communs (EUCC) (JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(6) Le règlement d'exécution (UE) 2024/482 ne précise pas la date jusqu'à laquelle la certification d'un produit TIC peut être fondée sur les versions précédentes des normes relatives aux critères communs et à la méthode d'évaluation commune. Les domaines techniques et les profils de protection énumérés aux annexes I, II et III dudit règlement d'exécution sont fondés sur des versions précédentes des normes ISO/CEI 15408 et 18045. Le règlement d'exécution (UE) 2024/482 devrait donc préciser, d'une part, les circonstances dans lesquelles la version précédente des critères communs et de la méthode d'évaluation commune continue de s'appliquer et, d'autre part, la manière dont la transition vers la version la plus récente des normes internationales s'effectuera.

(7) Au cours de la période de transition, la mise à jour des domaines techniques et des profils de protection pertinents devrait constituer une priorité pour les parties prenantes concernées. Le règlement d'exécution (UE) 2024/482 devrait prévoir que les cibles de sécurité fondées sur une version précédente des normes seraient acceptées jusqu'au 31 décembre 2027, conformément à la politique de transition adoptée par le CCRA. Il convient toutefois de noter que la politique de transition du CCRA couvre les évaluations initiales des produits et des profils de protection entamées au plus tard le 30 juin 2024, date à laquelle le schéma EUCC n'était pas encore applicable. Par ailleurs, conformément à la politique de transition du CCRA, le règlement d'exécution (UE) 2024/482 devrait prévoir que les cibles de sécurité conformes audit règlement d'exécution et déclarées conformes aux profils de protection fondés sur une version précédente des normes peuvent être acceptées jusqu'au 31 décembre 2027. En outre, lorsqu'un nouveau certificat est délivré en vertu du règlement d'exécution (UE) 2024/482 dans le cadre du processus de réexamen d'un certificat national qui démarre dans un délai de deux ans à compter du certificat initial, il devrait être possible d'utiliser une version précédente des normes. Cette possibilité serait dénuée de pertinence lorsqu'un processus de réexamen n'exige pas la délivrance d'un nouveau certificat en vertu du règlement d'exécution (UE) 2024/482 et lorsque le certificat reste valable.

(8) Afin de garantir une transition ordonnée vers la version la plus récente des normes, le règlement d'exécution (UE) 2024/482 devrait prévoir des règles transitoires spécifiques et continuer d'autoriser la délivrance de certificats au titre dudit règlement d'exécution attestant la conformité avec les profils de protection qui sont fondés sur des versions antérieures des normes publiées par le CCRA lorsque l'utilisation de tels profils de protection est requise en vertu de la législation de l'Union. C'est le cas pour le règlement d'exécution (UE) 2016/799 de la Commission ([3]), le règlement (UE) n° 910/2014 du Parlement européen et du Conseil ([4]) et la décision d'exécution (UE) 2016/650 de la Commission ([5]).

(9) L'annexe I du règlement d'exécution (UE) 2024/482 énumère les documents de référence applicables pour l'évaluation des produits TIC et des profils de protection. Elle ne précise cependant pas la version de ces documents. Il convient donc de préciser quelle est la version des documents qui s'applique aux certificats délivrés au titre du schéma EUCC. Ces versions s'appuient sur des documents approuvés par le groupe européen de certification de cybersécurité (GECC) et ont fait l'objet d'un réexamen plus approfondi en vue de leur inclusion dans le schéma EUCC. En outre, il y a lieu de modifier l'annexe I afin d'y inclure les documents de référence nouveaux ou mis à jour après leur approbation par le GECC, garantissant ainsi une accréditation uniforme des organismes d'évaluation de la conformité dans le cadre du schéma EUCC. Les exigences relatives à l'accréditation des CESTI devraient être mises à jour pour clarifier l'application des critères d'indépendance et d'impartialité, et un nouveau document de référence devrait être élaboré pour l'accréditation des organismes de certification.

(10) Des documents de référence sont susceptibles d'être ajoutés au schéma EUCC ou de faire l'objet de mises à jour dans le cadre des activités relatives au maintien du schéma. Pour les documents de référence nouveaux ou mis à jour, il pourrait être nécessaire d'établir des règles transitoires appropriées pour permettre aux vendeurs, aux CESTI, aux organismes de certification et aux autres parties prenantes de procéder aux adaptations nécessaires. En ce qui concerne la mise à jour du document de référence relatif à l'accréditation des CESTI, le document mis à jour ne devrait s'appliquer aux accréditations délivrées avant le 8 juillet 2025 que lorsqu'elles font l'objet d'un réexamen, comme c'est le cas dans le cadre d'une procédure d'évaluation ou de réévaluation. En outre, le document mis à jour devrait s'appliquer à toutes les accréditations de CESTI délivrées après le 8 juillet 2025.

([3]) Règlement d'exécution (UE) 2016/799 de la Commission du 18 mars 2016 mettant en œuvre le règlement (UE) n° 165/2014 du Parlement européen et du Conseil en ce qui concerne les exigences applicables à la construction, aux essais, à l'installation, à l'utilisation et à la réparation des tachygraphes et de leurs composants (JO L 139 du 26.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

([4]) Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([5]) Décision d'exécution (UE) 2016/650 de la Commission du 25 avril 2016 établissant des normes relatives à l'évaluation de la sécurité des dispositifs qualifiés de création de signature électronique et de cachet électronique conformément à l'article 30, paragraphe 3, et à l'article 39, paragraphe 2, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (JO L 109 du 26.4.2016, p. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).

(11) Il convient par ailleurs de rectifier les articles 5, 8, 16, 29 et 44 et l'annexe IV du règlement d'exécution (UE) 2024/482 afin de contribuer à garantir une formulation uniforme et une interprétation juridique claire.

(12) Les règles relatives aux notifications des organismes d'évaluation de la conformité devraient être établies horizontalement pour tous les schémas relevant du cadre européen de certification de cybersécurité. Les règles relatives à ces notifications relèvent du règlement d'exécution (UE) 2024/3143 de la Commission ([6]). Par conséquent, il y a lieu de supprimer les articles 23 et 24 du règlement d'exécution (UE) 2024/482 à partir de la date d'application du règlement d'exécution (UE) 2024/3143.

(13) Il convient donc de modifier et de rectifier en conséquence le règlement d'exécution (UE) 2024/482.

(14) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 66 du règlement (UE) 2019/881,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

*Article premier*

Le règlement d'exécution (UE) 2024/482 est modifié comme suit:

1) À l'article 2, les points 1) et 2) sont remplacés par le texte suivant:

«1) "critères communs": les critères communs pour l'évaluation de la sécurité des technologies de l'information, tels qu'ils figurent dans les normes ISO/CEI 15408-1:2022, ISO/CEI 15408-2:2022, ISO/CEI 15408-3:2022, ISO/CEI 15408-4:2022 ou ISO/CEI 15408-5:2022, ou les critères communs pour l'évaluation de la sécurité des technologies de l'information, version CC:2022, parties 1 à 5, publiés par les participants à l'accord de reconnaissance des certificats Critères Communs dans le domaine de la sécurité informatique;

2) "méthode d'évaluation commune": la méthode commune pour l'évaluation de la sécurité des technologies de l'information, telle qu'elle figure dans la norme ISO/CEI 18045:2022, ou la méthode commune pour l'évaluation de la sécurité des technologies de l'information, version CEM:2022, publiée par les participants à l'accord de reconnaissance des certificats Critères Communs dans le domaine de la sécurité informatique;».

2) L'article 3 est remplacé par le texte suivant:

«*Article 3*

**Normes d'évaluation**

1. Les normes suivantes s'appliquent aux évaluations réalisées dans le cadre du schéma EUCC:

a) les critères communs;

b) la méthode d'évaluation commune.

2. Jusqu'au 31 décembre 2027, un certificat peut être délivré au titre du schéma EUCC en appliquant l'une des normes suivantes:

a) ISO/CEI 15408-1:2009, ISO/CEI 15408-2:2008 ou ISO/CEI 15408-3:2008;

b) les critères communs pour l'évaluation de la sécurité des technologies de l'information, version 3.1, révision 5, publiés par les participants à l'accord de reconnaissance des certificats Critères Communs dans le domaine de la sécurité informatique;

([6]) Règlement d'exécution (UE) 2024/3143 de la Commission du 18 décembre 2024 établissant les circonstances, formats et procédures pour les notifications en application de l'article 61, paragraphe 5, du règlement (UE) 2019/881 du Parlement européen et du Conseil relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications (JO L, 2024/3143, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

c) ISO/CEI 18045:2008;

d) la méthode commune pour l'évaluation de la sécurité des technologies de l'information, révision 5, version 3.1, publiée par les participants à l'accord de reconnaissance des certificats Critères Communs dans le domaine de la sécurité informatique.

3. Jusqu'au 31 décembre 2027, un certificat qui applique les normes mentionnées au paragraphe 1 peut être délivré au titre du schéma EUCC et attester la conformité avec un profil de protection qui a appliqué les normes énumérées au paragraphe 2.

4. Un certificat qui applique les normes mentionnées au paragraphe 1 peut également être délivré au titre du schéma EUCC et attester la conformité avec un profil de protection qui a appliqué l'une des normes suivantes, à condition que l'utilisation de ce profil de protection soit requise en vertu du règlement d'exécution (UE) 2016/799 de la Commission (*), du règlement (UE) nº 910/2014 du Parlement européen et du Conseil (**) ou de la décision d'exécution (UE) 2016/650 de la Commission (***):

a) les critères communs pour l'évaluation de la sécurité des technologies de l'information, version 3.1, révisions 1 à 4, publiés par les participants à l'accord de reconnaissance des certificats Critères Communs dans le domaine de la sécurité informatique;

b) la méthode commune pour l'évaluation de la sécurité des technologies de l'information, version 3.1, révisions 1 à 4, publiée par les participants à l'accord de reconnaissance des certificats Critères Communs dans le domaine de la sécurité informatique.

_____

(*) Règlement d'exécution (UE) 2016/799 de la Commission du 18 mars 2016 mettant en œuvre le règlement (UE) nº 165/2014 du Parlement européen et du Conseil en ce qui concerne les exigences applicables à la construction, aux essais, à l'installation, à l'utilisation et à la réparation des tachygraphes et de leurs composants (JO L 139 du 26.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

(**) Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(***) Décision d'exécution (UE) 2016/650 de la Commission du 25 avril 2016 établissant des normes relatives à l'évaluation de la sécurité des dispositifs qualifiés de création de signature électronique et de cachet électronique conformément à l'article 30, paragraphe 3, et à l'article 39, paragraphe 2, du règlement (UE) nº 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (JO L 109 du 26.4.2016, p. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).».

3) Au chapitre IV, l'article 20 *bis* suivant est inséré:

«*Article 20 bis*

**Spécification des exigences relatives à l'accréditation des organismes d'évaluation de la conformité**

L'accréditation des organismes d'évaluation de la conformité tient compte de la spécification des exigences relatives à l'accréditation des organismes de certification et des CESTI, telle qu'elle figure dans les documents de référence applicables énumérés à l'annexe I, point 2.».

4) Les articles 23 et 24 sont supprimés.

5) À l'article 48, le paragraphe 4 suivant est ajouté:

«4. Sauf disposition contraire de l'annexe I ou de l'annexe II, les documents de référence s'appliquent à compter de la date d'application de l'acte modificatif par lequel ils ont été inclus dans l'annexe I ou l'annexe II.».

6) À l'article 49, le paragraphe 4 suivant est ajouté:

«4. Lorsqu'il est procédé au réexamen mentionné au paragraphe 3 dans un délai de deux ans à compter de la délivrance du certificat initial et lorsqu'un tel réexamen donne lieu à la délivrance d'un nouveau certificat conformément au présent règlement, les normes énumérées à l'article 3, paragraphe 2, peuvent être appliquées. La date de délivrance du certificat initial s'entend comme la date de délivrance du dernier certificat pour un produit TIC ou un profil de protection sur lequel se fonde la certification en cours de validité.».

7) L'annexe I est remplacée par le texte figurant à l'annexe I du présent règlement.

8) L'annexe IV est modifiée conformément à l'annexe II du présent règlement.

*Article 2*

Le règlement d'exécution (UE) 2024/482 est rectifié comme suit:

1) À l'article 5, paragraphe 1, le point b) est remplacé par le texte suivant:

«b) déclarée conforme à un profil de protection certifié dans le cadre du processus TIC, lorsque le produit TIC relève de la catégorie de produits TIC couverte par ce profil de protection.».

2) L'article 8 est rectifié comme suit:

a) le titre est remplacé par le texte suivant:

«Informations nécessaires pour la certification et l'évaluation»;

b) le paragraphe 1 est remplacé par le texte suivant:

«1. Un candidat à la certification EUCC fournit ou met à la disposition de l'organisme de certification et du CESTI toutes les informations nécessaires pour les activités de certification et d'évaluation.».

3) L'article 16 est remplacé par le texte suivant:

«*Article 16*

**Informations nécessaires pour la certification et l'évaluation des profils de protection**

Le candidat à la certification d'un profil de protection fournit ou met à la disposition de l'organisme de certification et du CESTI toutes les informations nécessaires pour les activités de certification et d'évaluation, sous une forme complète et correcte. L'article 8, paragraphes 2, 3, 4 et 7, s'applique mutatis mutandis.».

4) À l'article 17, le paragraphe 1 est supprimé.

5) À l'article 29, le paragraphe 2 est remplacé par le texte suivant:

«2. Si le titulaire du certificat EUCC ne propose pas de mesure corrective appropriée au cours du délai prévu au paragraphe 1, le certificat est suspendu conformément à l'article 30 ou retiré conformément à l'article 14 ou à l'article 20.».

*Article 3*

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

L'article 1er, paragraphe 4, s'applique à partir du 8 janvier 2025.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 18 décembre 2024.

*Par la Commission*
*La présidente*
Ursula VON DER LEYEN

*ANNEXE I*

*««ANNEXE I*

**Documents de référence à l'appui des domaines techniques et autres documents de référence**

1. Documents de référence à l'appui des domaines techniques au niveau AVA_VAN 4 ou 5:

   a) les documents suivants relatifs à l'évaluation harmonisée du domaine technique "cartes à puce et dispositifs similaires":

      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) les documents suivants relatifs à l'évaluation harmonisée du domaine technique "dispositifs matériels avec boîtiers de sécurité":

      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. Documents de référence relatifs à l'accréditation harmonisée des organismes d'évaluation de la conformité:

   a) "Accreditation of ITSEFs for the EUCC", version 1.1 pour les accréditations délivrées avant le 8 juillet 2025;

   b) "Accreditation of ITSEFs for the EUCC", version 1.6c pour les accréditations récemment délivrées ou révisées après le 8 juillet 2025;

   c) "Accreditation of CBs for the EUCC", version 1.6b.».».

*ANNEXE II*

À l'annexe IV, section IV.3, du règlement d'exécution (UE) 2024/482, les points 5 et 6 sont remplacés par le texte suivant:

«5. Lorsque les modifications sont considérées comme mineures par l'organisme de certification, aucun nouveau certificat n'est délivré pour le produit TIC modifié et un rapport de maintenance du rapport de certification initial est établi.

Le rapport de maintenance est inclus comme un sous-ensemble du rapport d'analyse d'impact et contient les sections suivantes:

a) introduction;

b) description des modifications;

c) éléments de preuve du développeur concerné.

6. Le rapport de maintenance mentionné au point 5 est fourni à l'ENISA pour publication sur son site web de certification de cybersécurité.».