Journal officiel
de l'Union européenne

FR
Série L

2025/2462

9.12.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/2462 DE LA COMMISSION

du 8 décembre 2025

modifiant le règlement d'exécution (UE) 2024/482 en ce qui concerne les définitions, la certification de séries de produits TIC, la continuité de l'assurance et les documents de référence

(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 fondé sur des critères communs (EUCC), conformément au cadre européen de certification de cybersécurité défini dans le règlement (UE) 2019/881.

(2) La méthode d'évaluation commune accompagnant les critères communs (CC), qui constitue une norme internationale pour l'évaluation de la sécurité des technologies de l'information, permet d'évaluer la sécurité des produits TIC aux fins de leur certification. Dans ce contexte, certains produits TIC peuvent s'appuyer sur la même base fonctionnelle afin d'offrir des fonctionnalités de sécurité similaires sur différentes plateformes ou appareils, et constituent alors ce que l'on appelle une «série de produits». Toutefois, la conception, le matériel, les micrologiciels ou les logiciels peuvent varier d'un produit TIC à l'autre. Il appartient à l'organisme de certification de décider au cas par cas s'il est possible d'effectuer la certification d'une série de produits. Les lignes directrices de l'EUCC y afférentes pourraient illustrer plus en détail les conditions de certification des séries de produits.

(3) Afin de préserver la fiabilité des produits certifiés, il est essentiel de définir ce qui constitue une modification majeure ou mineure de la cible d'évaluation ou de son environnement, y compris son environnement opérationnel ou de développement. Par conséquent, il est nécessaire de préciser ces notions en tenant compte des spécifications techniques existantes et largement utilisées du groupe des hauts fonctionnaires pour la sécurité des systèmes d'information (SOG-IS) et des participants à l'Accord de reconnaissance des certificats Critères Communs dans le domaine de la sécurité informatique (CCRA).

(4) Les modifications mineures se caractérisent souvent par leur incidence limitée sur la déclaration d'assurance produit fournie par le certificat EUCC délivré. Par conséquent, les modifications mineures devraient être gérées dans le cadre de procédures de maintenance et ne nécessitent pas de réévaluation des fonctionnalités de sécurité du produit. Parmi les exemples de modifications mineures qu'il convient de traiter dans le cadre de la maintenance figurent, sans toutefois s'y limiter, les modifications rédactionnelles, les modifications de l'environnement de la cible d'évaluation qui ne modifient pas la cible d'évaluation certifiée et les modifications de la cible d'évaluation certifiée qui n'ont pas d'incidence sur les éléments de preuve de l'assurance. Les modifications de l'environnement de développement peuvent également être considérées comme mineures, pour autant qu'elles soient sans effet sur les mesures d'assurance existantes. Elles peuvent toutefois, dans certains cas, nécessiter une évaluation partielle des mesures concernées.

([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).

(5) Une modification majeure désigne toute modification de la cible d'évaluation certifiée ou de son environnement qui est susceptible d'avoir une incidence négative sur l'assurance indiquée dans le certificat EUCC, de sorte qu'elle devrait nécessiter une réévaluation. Parmi les exemples de modifications majeures figurent, sans toutefois s'y limiter, les modifications de l'ensemble des exigences en matière d'assurance déclarée, à l'exception des exigences en matière d'assurance de la famille de CC ALC_FLR (correction des anomalies); les modifications des contrôles de confidentialité ou d'intégrité de l'environnement de développement lorsque ces modifications pourraient avoir une incidence sur la sécurité du développement ou de la production de la cible d'évaluation, ou les modifications de la cible d'évaluation visant à remédier à une vulnérabilité exploitable. En outre, un ensemble de modifications mineures ayant collectivement une incidence significative sur la sécurité peut aussi être qualifié de modification majeure. Il importe également de reconnaître que si la correction d'un bogue peut n'affecter qu'un aspect spécifique de la cible d'évaluation, son imprévisibilité et son incidence potentielle sur l'assurance peuvent en faire une modification majeure si elle compromet les assurances de sécurité fournies par la certification.

(6) Les modifications de l'environnement de menaces d'un produit TIC certifié inchangé pourraient nécessiter une réévaluation. Les résultats possibles d'un tel processus de réévaluation, en particulier son incidence sur le certificat EUCC, devraient être clairement établis. Si une réévaluation est concluante, l'organisme de certification devrait confirmer le certificat ou délivrer un nouveau certificat avec une nouvelle date d'expiration. Si un processus de réévaluation n'est pas concluant, l'organisme de certification devrait retirer le certificat et éventuellement délivrer un nouveau certificat avec un champ d'application différent. Ces dispositions devraient s'appliquer mutatis mutandis à la réévaluation des profils de protection.

(7) 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. Ces documents de référence devraient être mis à jour pour tenir compte des dernières évolutions, telles que celles liées aux technologies, au panorama des cybermenaces, aux pratiques du secteur ou aux normes internationales. Cette mise à jour se révèle opportune pour les documents de référence relatifs aux exigences minimales de sécurité du site, à l'application de potentiels d'attaque aux cartes à puce, à l'application de potentiels d'attaque aux dispositifs matériels avec boîtiers de sécurité, à l'application de critères communs aux circuits intégrés et à l'évaluation de produit composite pour les cartes à puce et dispositifs similaires. Par ailleurs, les documents de référence liés à l'évaluation et à la certification de produit composite utilisant la dernière version des normes CC, à la réutilisation des résultats de l'évaluation des audits sur place et aux clarifications concernant l'interprétation des profils de protection relatifs aux dispositifs de création de signature électronique qualifiés, aux tachygraphes et aux modules de sécurité matériels ne sont pas inclus. Afin de garantir une évaluation uniforme des produits TIC au titre de l'EUCC, 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 groupe européen de certification de cybersécurité (GECC).

(8) En outre, le document de référence intitulé «ADV_SPM.1 interpretation for [CC:2022] transition» devrait être ajouté au schéma afin de veiller à ce que les processus de certification reposant sur des profils de protection spécifiques puissent continuer à utiliser la modélisation formelle (ADV_SPM.1) jusqu'à ce que les profils de protection correspondants soient mis à jour, par exemple avec l'ajout d'une configuration de profils de protection multi-assurance conformes aux CC:2022 qui prend en charge l'ADV_SPM.1. Afin de laisser suffisamment de temps aux acteurs du marché pour passer aux normes CC actualisées, il convient de prévoir des règles de transition spécifiques pour les profils de protection BSI-CC-PP-0084-2014 [«Security IC Platform PP with Augmentation Packages (v1.0)»], BSI-CC-PP-0101-V2-2020 [«Java Card System – Closed Configuration (v3.1)»], ou BSI-CC-PP-0099-V2-2020 [«Java Card System – Open Configuration (v3.1)»]. Afin d'éviter toute perturbation du marché, il convient d'établir que le document de référence sur l'interprétation de l'ADV_SPM.1 pour la transposition en CC:2022 s'applique aux processus de certification qui ont été lancés avant l'adoption du présent règlement. L'application de ce document devrait toutefois être limitée au strict nécessaire, compte tenu du temps nécessaire pour finaliser la mise à jour des profils de protection correspondants. Plus précisément, pour les processus de certification utilisant les profils de protection BSI-CC-PP-0084-2014 [«Security IC Platform PP with Augmentation Packages (v1.0)»] ou BSI-CC-PP-0101-V2-2020 [«Java Card System – Closed Configuration (v3.1)»], le document de référence devrait s'appliquer aux processus qui ont été lancés avant le 1er octobre 2026. Pour les processus de certification utilisant le profil de protection BSI-CC-PP-0099-V2-2020 [«Java Card System – Open Configuration (v3.1)»], le document de référence ne devrait s'appliquer qu'aux processus lancés avant la date d'entrée en vigueur du présent règlement, étant donné qu'une nouvelle version dudit profil de protection est déjà disponible.

(9) Une modification des documents de référence au cours d'un processus de certification pourrait perturber l'évaluation du produit et retarder la délivrance du certificat. Par conséquent, pour les documents de référence nouveaux ou mis à jour, il est 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. Les documents de référence nouveaux et mis à jour applicables devraient concerner les demandes de certification, y compris les demandes de réévaluation, tandis qu'il devrait être possible de continuer à utiliser des versions antérieures des documents de référence pour les processus de certification en cours.

(10) Les annexes II et III du règlement d'exécution (UE) 2024/482 énumèrent, respectivement, les profils de protection certifiés au niveau AVA_VAN 4 ou 5 et les profils de protection recommandés. Les profils de protection ayant été mis à jour, plusieurs références sont désormais incomplètes ou obsolètes. Ces références devraient être complétées et, par ailleurs, de nouvelles références devraient être incluses afin de garantir une couverture plus complète des circuits intégrés sécurisés, des cartes à puce et dispositifs similaires, et des systèmes informatiques de confiance.

(11) Il est nécessaire d'apporter des modifications à l'article 19 du règlement d'exécution (UE) 2024/482 afin de préciser que l'annexe IV s'applique, avec les modifications nécessaires, au réexamen des certificats EUCC pour les profils de protection.

(12) Étant donné que la cible de sécurité est un élément essentiel pour comprendre la portée d'un processus de certification, il est également nécessaire que l'ENISA publie sur son site internet la cible de sécurité correspondant à chaque certificat EUCC.

(13) En outre, les organismes de certification devraient fournir à l'ENISA une version anglaise de la cible de sécurité et du rapport de certification afin que l'agence puisse mettre à disposition ces informations en anglais sur le site internet correspondant, conformément à l'article 42, paragraphe 2, du règlement d'exécution (UE) 2024/482. C'est pourquoi les candidats à la certification devraient fournir aux organismes de certification une version anglaise de la cible de sécurité, chaque fois que cela leur est demandé.

(14) Il n'est pas nécessaire que la référence au nom de l'organisme de certification figure dans l'identifiant unique du certificat, étant donné que le numéro d'identification de l'organisme de certification est suffisant pour identifier cet organisme de manière unique. Le mois de délivrance ne doit pas apparaître non plus, étant donné que le comptage des certificats est effectué sur une base annuelle. Cette exigence devrait donc être supprimée à des fins de simplification. Étant donné que l'année de délivrance du certificat correspond à la délivrance du premier certificat, cette même date devrait être incluse dans l'identifiant unique qui figure sur les certificats délivrés après un réexamen, afin de garantir la traçabilité.

(15) Il convient dès lors de modifier le règlement d'exécution (UE) 2024/482 en conséquence.

(16) 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 16), 17) et 18) suivants sont ajoutés:

«16) "série de produits": un ensemble de produits TIC par un candidat, s'appuyant sur la même base fonctionnelle afin de répondre aux mêmes besoins de sécurité, dont la conception, le matériel, les micrologiciels ou les logiciels peuvent varier d'un produit TIC à l'autre;

17) "modification majeure": toute modification de la cible d'évaluation certifiée ou de son environnement qui n'a aucune incidence négative sur l'assurance indiquée dans le certificat EUCC;

18) "modification majeure": toute modification de la cible d'évaluation certifiée ou de son environnement qui est susceptible d'avoir une incidence négative sur l'assurance indiquée dans le certificat EUCC.».

2) À l'article 5, le paragraphe 3 suivant est ajouté:

«3. Un organisme de certification peut autoriser la certification d'une série de produits.».

3) À l'article 9, paragraphe 2, le point a) est remplacé par le texte suivant:

«a) fournir à l'organisme de certification et au CESTI toutes les informations nécessaires, complètes et correctes, et fournir les informations supplémentaires nécessaires si elles lui sont demandées, y compris une version anglaise de la cible de sécurité;».

4) À l'article 11, paragraphe 3, le point b) est remplacé par le texte suivant:

«b) l'identifiant unique du certificat, comprenant:

1) le nom du schéma;

2) le numéro d'identification, conformément à l'article 3 du règlement d'exécution (UE) 2024/3143, de l'organisme de certification qui a délivré le certificat;

3) l'année de délivrance du certificat initial;

4) le numéro d'identification assigné par l'organisme de certification qui a délivré le certificat.».

5) À l'article 19, le paragraphe 1 est remplacé par le texte suivant:

«1. À la demande du titulaire du certificat ou pour d'autres raisons justifiées, l'organisme de certification peut décider de réexaminer le certificat EUCC d'un profil de protection. Le réexamen est effectué conformément à l'annexe IV. L'organisme de certification détermine l'étendue du réexamen. Lorsque c'est nécessaire aux fins du réexamen, l'organisme de certification demande au CESTI de réévaluer le profil de protection certifié.».

6) L'article 42 est modifié comme suit:

a) au paragraphe 1, le point i) suivant est ajouté:

«i) la cible de sécurité correspondant à chaque certificat EUCC;»;

b) le paragraphe 2 est remplacé par le texte suivant:

«2. Les informations visées au paragraphe 1 sont mises à disposition au moins en anglais. À cette fin, les organismes de certification fournissent à l'ENISA les versions linguistiques originales des rapports de certification et des cibles de sécurité, ainsi que la version anglaise de ces documents sans retard injustifié.».

7) À l'article 48, le paragraphe 4 est remplacé par le texte suivant:

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

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

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

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

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

12) L'annexe V est modifiée conformément à l'annexe V du présent règlement.

13) L'annexe IX est remplacée par le texte figurant à l'annexe VI du présent règlement.

Article 2

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

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

Fait à Bruxelles, le 8 décembre 2025.

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 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, d'application pour les processus de certification utilisant les profils de protection suivants:

         a) BSI-CC-PP-0084-2014 ["Security IC Platform PP with Augmentation Packages (v1.0)"], ou BSI-CC-PP-0101-V2-2020 ["Java Card System – Closed Configuration (v3.1)"], initiés avant le 1er octobre 2026;

         b) BSI-CC-PP-0099-V2-2020 ["Java Card System – Open Configuration (v3.1)"], initié avant le 29 décembre 2025;

   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 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) 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

«*ANNEXE II*

Profils de protection certifiés au niveau AVA_VAN 4 ou 5

1) Pour les dispositifs de création de signature ou de cachet électronique qualifiés à distance:

   a) EN 419241-2:2019 - Systèmes fiables de serveur de signature électronique - Partie 2: profil de protection de QSCD pour la signature par serveur (v0.16), ANSSI-CC-PP-2018/02-M01;

   b) EN 419221-5:2018 - Profils de protection pour les modules cryptographiques de prestataires de services de confiance - Partie 5: module cryptographique pour les services de confiance (v0.15), ANSSI-CC-PP-2016/05-M01.

2) Profils de protection adoptés en tant que documents de référence:

   [VIERGE].».

ANNEXE III

«*ANNEXE III*

Profils de protection recommandés

Profils de protection utilisés dans la certification des produits TIC, y compris les produits dans les domaines techniques énumérés ci-dessous.

1) Cartes à puce et dispositifs similaires

   a) Passeport:

      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) Dispositifs sécurisés de création de signature (SSCD):

      1) EN 419211-2:2013 – Profils de protection des dispositifs sécurisés de création de signature – Partie 2: dispositif avec génération de clé (v1.03), BSI-CC-PP-0059-2009-MA-02;

      2) EN 419211-3:2013 – Profils de protection des dispositifs sécurisés de création de signature – Partie 3: dispositif avec import de clé (v1.0.2), BSI-CC-PP-0075-2012-MA-01;

      3) EN 419211-4:2013 – Profils de protection pour dispositif sécurisé de création de signature électronique - Partie 4: extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de génération de certificats (v1.0.1), BSI-CC-PP-0071-2012-MA-01;

      4) EN 419211-5:2013 – Profils de protection pour dispositif sécurisé de création de signature - Partie 5: extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de création de signature (v1.0.1), BSI-CC-PP-0072-2012-MA-01;

      5) EN 419211-6:2014 – Profils de protection pour dispositif sécurisé de création de signature électronique - Partie 6: extension pour un dispositif avec import de clé et communication sécurisée avec l'application de création de signature (v1.0.4), BSI-CC-PP-0076-2013-MA-01.

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

   d) CI sécurisés, plateforme Java Card et 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 (TPM): 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) Dispositifs matériels avec boîtier de sécurité

   a) Points d'interaction (de paiement) et terminaux de paiement (POI):

      1) Point d'interaction "POI-CHIP-ONLY" (v4.0), ANSSI-CC-PP-2015/01;

      2) Point d'interaction "POI-CHIP-ONLY and Open Protocol Package" (v4.0), ANSSI-CC-PP-2015/02;

      3) Point d'interaction "POI-COMPREHENSIVE" (v4.0), ANSSI-CC-PP-2015/03;

      4) Point d'interaction "POI-COMPREHENSIVE and Open Protocol Package" (v4.0), ANSSI-CC-PP-2015/04;

      5) Point d'interaction "POI-PED-ONLY" (v4.0), ANSSI-CC-PP-2015/05;

      6) Point d'interaction "POI-PED-ONLY and Open Protocol Package" (v4.0), ANSSI-CC-PP-2015/06.

   b) Module de sécurité matériel:

      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) Tachygraphe:

      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) Autres: Trusted Execution Environment Protection Profile – GPD_SPE_021 (v1.3), ANSSI-CC-PP-2014/01-M02.».

ANNEXE IV

L'annexe IV du règlement d'exécution (UE) 2024/482 est modifiée comme suit:

1) Au point IV.2, le point 4 est remplacé par le texte suivant:

«4. L'organisme de certification examine le rapport technique d'évaluation mis à jour et établit un rapport de réévaluation. Le statut du certificat initial est alors modifié conformément à l'article 13 ou à l'article 19. Si le processus de réévaluation est concluant, l'article 13, paragraphe 2, point a) ou c), s'applique dans le cas de la certification d'un produit et l'article 19, paragraphe 2, point a) ou c), s'applique dans le cas de la certification d'un profil de protection. Si le processus de réévaluation n'est pas concluant, l'article 13, paragraphe 2, point a) ou d), s'applique dans le cas de la certification d'un produit et l'article 19, paragraphe 2, point b) ou d), s'applique dans le cas de la certification d'un profil de protection.».

2) Le point IV.3 est modifié comme suit:

a) le titre IV.3 est remplacé par le texte suivant:

«IV.3 **Modification d'un produit TIC certifié – Maintenance et réévaluation»;**

b) les points 4 et 5 sont remplacés par le texte suivant:

«4. À l'issue de l'examen, l'organisme de certification détermine si l'ampleur d'une modification est mineure ou majeure en fonction de son incidence sur l'assurance indiquée dans le certificat EUCC.

5. Lorsque les modifications sont considérées comme mineures par l'organisme de certification, aucun nouveau certificat n'est délivré pour le produit TIC modifié conformément à l'article 13, paragraphe 2, point a), ou à l'article 19, paragraphe 2, point a), et un rapport de maintenance du rapport de certification initial est établi.»;

c) le point 5 *bis* suivant est inséré:

«5 *bis*. En cas de modification des mesures d'assurance dans l'environnement de développement, y compris l'ajout d'exigences en matière d'assurance de la famille de CC ALC_FLR (correction des anomalies), l'organisme de certification peut demander au CESTI de procéder à l'évaluation d'un sous-ensemble des mesures d'assurance concernées. Le CESTI publie un rapport technique d'évaluation partielle, sur la base duquel l'organisme de certification confirme que les modifications sont mineures ou majeures. Lorsque l'organisme de certification confirme que les modifications sont mineures, le point IV.3, 5, s'applique. Lorsque l'organisme de certification confirme que les modifications sont majeures, le point IV.3, 7, s'applique.».

ANNEXE V

Le point V.1 de l'annexe V du règlement d'exécution (UE) 2024/482 est remplacé par le texte suivant:

«V.1 **Rapport de certification**

1. Sur la base des rapports techniques d'évaluation fournis par le CESTI, l'organisme de certification établit un rapport de certification à publier avec le certificat EUCC et la cible de sécurité correspondants.

2. Le rapport de certification est une source d'informations détaillées et pratiques sur le produit TIC et sur le déploiement sécurisé du produit TIC. C'est pourquoi ce rapport inclut toutes les informations publiquement disponibles et partageables pertinentes pour les utilisateurs et les parties intéressées. Les informations publiquement disponibles et partageables peuvent être référencées dans le rapport de certification.

3. Le rapport de certification contient au moins les informations suivantes:

   a) un résumé;

   b) l'identification du produit TIC;

   c) les informations de contact concernant l'évaluation du produit TIC;

   d) les politiques de sécurité;

   e) les hypothèses et les éclaircissements quant au champ d'application;

   f) les informations architecturales;

   g) les informations supplémentaires sur la cybersécurité, le cas échéant;

   h) un résumé de l'évaluation du produit TIC et la configuration évaluée;

   i) les résultats de l'évaluation et les informations relatives au certificat;

   j) des observations et des recommandations, le cas échéant;

   k) des annexes, le cas échéant;

   l) une référence à la cible de sécurité du produit TIC soumis à la certification;

   m) le cas échéant, la marque ou l'étiquette associée au schéma;

   n) un glossaire, le cas échéant;

   o) une bibliographie.

4. Le résumé visé au paragraphe 3, point a), est une brève synthèse de l'ensemble du rapport de certification. Il fournit un aperçu clair et concis des résultats de l'évaluation et inclut les informations suivantes:

   a) le nom du produit TIC évalué;

   b) le nom du CESTI qui a réalisé l'évaluation;

   c) la date de fin de l'évaluation;

   d) la date de délivrance du certificat;

   e) le cas échéant, la date de délivrance du certificat initial;

   f) la période de validité;

   g) l'identifiant unique du certificat tel que décrit à l'article 11;

   h) une brève description des résultats du rapport de certification, y compris:

      i) la version et, le cas échéant, l'édition des critères communs appliqués à l'évaluation;

      ii) le paquet d'assurance ou la liste des composants d'assurance de sécurité des critères communs, y compris le niveau AVA_VAN appliqué pendant l'évaluation et le niveau d'assurance correspondant tel qu'énoncé à l'article 52 du règlement (UE) 2019/881 auquel le certificat EUCC fait référence;

      iii) le cas échéant, le ou les profils de protection avec lesquels le produit TIC revendique la conformité;

      iv) la référence à la politique de sécurité du produit TIC évalué;

      v) la ou les clauses de non-responsabilité, le cas échéant.

5. L'identification visée au paragraphe 3, point b), identifie clairement le produit TIC évalué, y compris en indiquant les informations suivantes:

   a) l'identifiant unique du produit TIC évalué;

   b) l'énumération des composants du produit TIC qui font partie de l'évaluation, avec le numéro de version de chaque composant;

   c) la référence aux exigences supplémentaires relatives à l'environnement opérationnel du produit TIC certifié.

6. Les coordonnées visées au paragraphe 3, point c), contiennent au moins les informations suivantes:

   a) le nom du développeur;

   b) le nom et les coordonnées du titulaire du certificat EUCC;

   c) le nom de l'organisme de certification qui a délivré le certificat;

   d) l'autorité nationale de certification de cybersécurité responsable;

   e) le nom du CESTI qui a réalisé l'évaluation et, le cas échéant, la liste des sous-traitants.

7. Les politiques de sécurité visées au paragraphe 3, point d), contiennent la description de la politique de sécurité du produit TIC en tant qu'ensemble de services de sécurité et les politiques ou règles que le produit TIC évalué met en œuvre ou auxquelles il se conforme. Elles contiennent également les informations suivantes:

   a) une description des procédures de gestion et de divulgation des vulnérabilités du titulaire du certificat, à compléter uniquement par des informations pouvant être mises à la disposition du public;

   b) la politique de continuité de l'assurance du titulaire du certificat, y compris, le cas échéant, la description des processus de production ou de gestion du cycle de vie du titulaire du certificat conformément à l'annexe IV, point IV.1;

   c) le cas échéant, la présence d'une procédure de gestion des correctifs et le résultat de son évaluation conformément à l'annexe IV, point IV.4.

8. Les hypothèses et les éclaircissements quant au champ d'application visés au paragraphe 3, point e), contiennent des informations concernant les circonstances et les objectifs liés à l'utilisation prévue du produit telle que visée à l'article 7, paragraphe 1, point c), et incluent les informations suivantes:

   a) des hypothèses sur l'utilisation et le déploiement du produit TIC sous la forme d'exigences minimales, telles que l'installation et la configuration correctes et la satisfaction des exigences en matière de matériel;

   b) des hypothèses sur l'environnement pour le fonctionnement conforme du produit TIC.

   c) une description de toute menace pour le produit TIC qui n'est pas prise en charge par les fonctions de sécurité évaluées du produit en fonction de l'utilisation prévue, si cela est jugé pertinent pour un utilisateur potentiel du produit TIC.

   Les informations énumérées au premier alinéa sont aussi claires et compréhensibles que possible afin que les utilisateurs potentiels du produit TIC certifié puissent prendre des décisions éclairées quant aux risques associés à son utilisation.

9. Les informations architecturales visées au paragraphe 3, point f), comprennent une description détaillée du produit TIC et de ses principaux composants, sur la base des éléments livrables définis dans les exigences en matière d'assurance de la famille de CC Development - TOE Design (ADV_TDS).

10. Les informations supplémentaires sur la cybersécurité visées au paragraphe 3, point g), comprennent le lien vers le site internet du titulaire du certificat EUCC visé à l'article 55 du règlement (UE) 2019/881.

11. L'évaluation et la configuration du produit TIC visées au paragraphe 3, point h), décrivent les efforts d'essais du développeur et de l'évaluateur, en décrivant l'approche, la configuration et l'ampleur des essais. Elles contiennent au moins les informations suivantes:

    a) l'identification des composants d'assurance utilisés dans les normes visées à l'article 3;

    b) la version des documents de référence et les autres critères d'évaluation de la sécurité utilisés dans l'évaluation;

    c) les paramètres et la configuration de la cible d'évaluation utilisés pour les essais et l'analyse de la vulnérabilité;

    d) tout profil de protection utilisé, y compris les informations suivantes: le nom du profil de protection, la version, la date et le certificat.

12. Les résultats de l'évaluation et les informations relatives au certificat visés au paragraphe 3, point i), comprennent des informations sur le niveau d'assurance atteint comme indiqué à l'article 4 du présent règlement et à l'article 52 du règlement (UE) 2019/881.

13. Les observations et recommandations visées au paragraphe 3, point j), sont utilisées pour communiquer des informations supplémentaires sur les résultats de l'évaluation. Ces observations et recommandations peuvent prendre la forme de lacunes du produit TIC découvertes au cours de l'évaluation ou de mentions de caractéristiques particulièrement utiles.

14. Les annexes visées au paragraphe 3, point k), sont utilisées pour décrire toute information supplémentaire qui pourrait être utile pour le public cible du rapport mais qui ne peuvent pas être logiquement incluses dans les sections prescrites du rapport, y compris dans les cas d'une description complète de la politique de sécurité.

15. La cible de sécurité visé au paragraphe 3, point l), mentionne la cible de sécurité évaluée. La cible de sécurité évaluée est accompagnée du rapport de certification aux fins de la publication sur le site internet visé à l'article 50, paragraphe 1, du règlement (UE) 2019/881. Lorsqu'un assainissement de la cible de sécurité évaluée s'impose avant la publication, il est effectué conformément à l'annexe V, point V.2, du présent règlement.

16. Les marques ou les étiquettes associées au schéma EUCC visées au paragraphe 3, point m), sont insérées dans le rapport de certification conformément aux règles et procédures prévues à l'article 11.

17. Le glossaire visé au paragraphe 3, point n), est utilisé pour faciliter la lecture du rapport au moyen de définitions d'acronymes ou de termes dont le sens peut ne pas ressortir clairement.

18. La bibliographie visée au paragraphe 3, point o), comprend les références à tous les documents utilisés pour l'élaboration du rapport de certification. Ces informations comprennent au moins les éléments suivants:

    a) les critères d'évaluation de la sécurité, les documents de référence et les autres spécifications pertinentes utilisées;

    b) le rapport technique d'évaluation;

    c) le rapport technique d'évaluation pour l'évaluation composite, le cas échéant;

    d) la documentation de référence technique;

    e) les orientations en matière de sécurité pour les développeurs;

    f) la liste de configuration pour les développeurs.

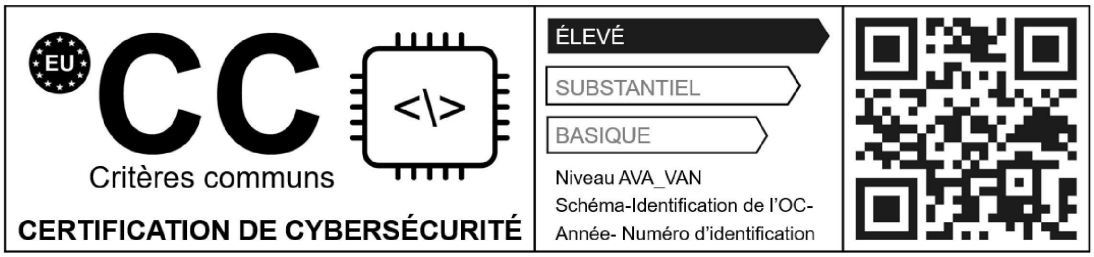
    Afin de garantir la possibilité de reproduire l'évaluation, toute la documentation à laquelle il est fait référence doit être identifiée de manière unique avec la date de publication et le numéro de version appropriés.».

ANNEXE VI

«ANNEXE IX

Marque et étiquette

1. Forme de la marque et de l'étiquette:



2. Si la marque et l'étiquette sont réduites ou agrandies, les proportions données au point 1 sont respectées.

3. Lorsqu'elles sont apposées physiquement sur le produit, la marque et l'étiquette ont une hauteur d'au moins 5 mm.».