Journal officiel
de l'Union européenne

FR
Série L

2024/482

7.2.2024

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)

(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 présent règlement 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. L'EUCC s'appuie sur l'accord de reconnaissance mutuelle (ARM) des certificats de sécurité des technologies de l'information du groupe des hauts fonctionnaires pour la sécurité des systèmes d'information ([2]) (SOG-IS) utilisant les critères communs, y compris les procédures et documents du groupe.

(2) Il convient que le schéma soit fondé sur des normes internationales établies. Les critères communs sont un ensemble de normes internationales pour l'évaluation de la sécurité de l'information publiées, par exemple, sous la référence ISO/IEC 15408 Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information. Ils reposent sur une évaluation par des tiers et prévoient sept niveaux d'assurance de l'évaluation (EAL). Les critères communs sont accompagnés de la méthode d'évaluation commune, publiée, par exemple, sous la référence ISO/IEC 18045 — Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information — Méthodologie pour l'évaluation de sécurité. Les spécifications et documents qui appliquent les dispositions du présent règlement peuvent se référer à une norme publiquement accessible qui reflète la norme utilisée pour la certification prévue par le présent règlement, telle que les critères communs pour l'évaluation de la sécurité des technologies de l'information et la méthodologie commune pour l'évaluation de la sécurité des technologies de l'information.

(3) L'EUCC utilise la famille d'évaluation de la vulnérabilité des critères communs (AVA_VAN), composants 1 à 5. Ces cinq composants fournissent les principaux déterminants et les principales dépendances pour l'analyse des vulnérabilités des produits TIC. Sachant que les composants correspondent aux niveaux d'assurance prévus dans le présent règlement, ils permettent de choisir l'assurance en connaissance de cause, sur la base des évaluations réalisées des exigences de sécurité et du risque associé à l'utilisation prévue du produit TIC. Le demandeur d'un certificat EUCC devrait fournir la documentation relative à l'utilisation prévue du produit TIC et à l'analyse des niveaux de risque associés à cette utilisation afin de permettre à l'organisme d'évaluation de la conformité d'évaluer l'adéquation du niveau d'assurance choisi. Lorsque les activités d'évaluation et de certification sont réalisées par le même organisme d'évaluation de la conformité, le demandeur ne devrait soumettre les informations demandées qu'une seule fois.

(4) Un domaine technique est un cadre de référence qui couvre un groupe de produits TIC ayant des fonctionnalités de sécurité spécifiques et similaires qui atténuent les attaques et dont les caractéristiques sont communes à un niveau d'assurance donné. Un domaine technique décrit dans des documents de référence les exigences de sécurité spécifiques ainsi que les méthodes, techniques et outils d'évaluation supplémentaires qui s'appliquent à la certification des produits TIC couverts par le domaine technique en question. Tout domaine technique favorise donc

([1]) JO L 151 du 7.6.2019, p. 15.

([2]) Accord de reconnaissance mutuelle des certificats d'évaluation de la sécurité des technologies de l'information, version 3.0 de janvier 2010, disponible sur sogis.eu, approuvé par le groupe de hauts fonctionnaires pour la sécurité des systèmes d'information de la Commission européenne en réponse au point 3 de la recommandation 95/144/CE du Conseil du 7 avril 1995 concernant des critères communs d'évaluation de la sécurité des technologies de l'information (JO L 93 du 26.4.1995, p. 27).

également l'harmonisation de l'évaluation des produits TIC couverts. Actuellement, deux domaines techniques sont largement utilisés pour la certification aux niveaux AVA_VAN.4 et AVA_VAN.5. Le premier domaine technique est celui des «cartes à puce et dispositifs similaires», où la fonctionnalité de sécurité requise dépend en grande partie d'éléments matériels spécifiques, adaptés et souvent séparables (par exemple, matériel de carte à puce, circuits intégrés, produits composites de carte à puce, modules de plateforme de confiance tels qu'utilisés dans les systèmes informatiques de confiance, ou cartes de tachygraphe numérique). Le deuxième domaine technique est celui des «dispositifs matériels avec boîtiers de sécurité», où la fonctionnalité de sécurité requise dépend en grande partie d'une enveloppe physique matérielle (appelée «boîtier de sécurité») conçue pour résister aux attaques directes, par exemple les terminaux de paiement, les unités de tachygraphe pour véhicules, les compteurs intelligents, les terminaux de contrôle d'accès et les modules de sécurité matériels.

(5) Lors d'une demande de certification, le demandeur devrait expliquer son choix de niveau d'assurance par rapport aux objectifs énoncés à l'article 51 du règlement (UE) 2019/881, et à la sélection de composants dans le catalogue des exigences fonctionnelles de sécurité et des exigences d'assurance de sécurité incluses dans les critères communs. Les organismes de certification devraient évaluer la pertinence du niveau d'assurance choisi et veiller à ce que le niveau choisi corresponde au niveau de risque associé à l'utilisation prévue du produit TIC.

(6) Selon les critères communs, la certification est effectuée par rapport à une cible de sécurité qui englobe une définition du problème de sécurité du produit TIC ainsi que les objectifs de sécurité qui répondent au problème de sécurité. Le problème de sécurité fournit des détails sur l'utilisation prévue du produit TIC et les risques associés à cette utilisation. Un ensemble sélectionné d'exigences de sécurité répond à la fois au problème de sécurité et aux objectifs de sécurité d'un produit TIC.

(7) Les profils de protection sont un moyen efficace de prédéterminer les critères communs applicables à une catégorie donnée de produits TIC et, par conséquent, un élément essentiel du processus de certification des produits TIC couverts par le profil de protection. Un profil de protection est utilisé pour évaluer les futures cibles de sécurité qui relèvent de la catégorie de produits TIC visée par ce profil de protection. Il permet de rationaliser et d'améliorer encore l'efficacité du processus de certification des produits TIC et aide les utilisateurs à spécifier correctement et efficacement la fonctionnalité d'un produit TIC. Les profils de protection devraient donc être considérés comme faisant partie intégrante du processus TIC menant à la certification des produits TIC.

(8) Afin de pouvoir jouer leur rôle dans le processus TIC soutenant le développement et la fourniture d'un produit TIC certifié, les profils de protection eux-mêmes devraient pouvoir être certifiés indépendamment de la certification du produit TIC spécifique qui relève du profil de protection en question. Il est donc essentiel d'appliquer au moins le même niveau de contrôle aux profils de protection qu'aux cibles de sécurité afin de garantir un niveau élevé de cybersécurité. Les profils de protection devraient être évalués et certifiés indépendamment du produit TIC correspondant et uniquement en appliquant la classe d'assurance des critères communs et de la méthode d'évaluation commune pour les profils de protection (APE) et, le cas échéant, pour les configurations de profils de protection (ACE). En raison de leur rôle important et sensible en tant que référence dans la certification des produits TIC, ils ne devraient être certifiés que par des organismes publics ou par un organisme de certification qui a reçu de l'autorité nationale de certification de cybersécurité l'approbation préalable pour le profil de protection concerné. Eu égard à leur rôle fondamental pour la certification au niveau d'assurance «élevé», notamment en dehors des domaines techniques, les profils de protection devraient être élaborés sous la forme de documents de référence à approuver par le groupe européen de certification de cybersécurité.

(9) Les profils de protection certifiés devraient être inclus dans le contrôle de conformité et de respect des règles de l'EUCC par les autorités nationales de certification de cybersécurité. Lorsque la méthodologie, les outils et les compétences appliqués aux approches concernant l'évaluation des produits TIC sont disponibles pour des profils de protection certifiés spécifiques, les domaines techniques pourraient être fondés sur ces profils.

(10) Afin d'assurer un niveau élevé de confiance et d'assurance dans les produits TIC certifiés, l'autoévaluation ne devrait pas être autorisée en vertu du présent règlement. Seule l'évaluation de la conformité par un tiers, à savoir un CESTI et un organisme de certification, devrait être autorisée.

(11) La communauté SOG-IS a fourni des interprétations et des approches communes pour l'application des critères communs et de la méthode d'évaluation commune à la certification, en particulier pour le niveau d'assurance «élevé» visé par les domaines techniques «cartes à puce et dispositifs similaires» et «dispositifs matériels avec boîtiers de sécurité». La réutilisation de ces documents d'appui dans le schéma EUCC garantit une transition en douceur entre les schémas SOG-IS mis en œuvre au niveau national et le schéma EUCC harmonisé. Par conséquent, il convient d'inclure dans le présent règlement des méthodes d'évaluation harmonisées applicables à l'ensemble des activités de certification. En outre, la Commission devrait pouvoir demander au groupe européen de certification de cybersécurité d'adopter un avis approuvant et recommandant l'application des méthodes d'évaluation spécifiées dans les documents de référence pour la certification de produit TIC ou de profil de protection dans le cadre du schéma EUCC. Par conséquent, le présent règlement énumère à l'annexe I les documents de référence relatifs aux activités d'évaluation menées par les organismes d'évaluation de la conformité. Le groupe européen de certification de cybersécurité devrait approuver et tenir à jour les documents de référence. Les documents de référence devraient être utilisés pour la certification. Ce n'est que dans des cas exceptionnels et dûment justifiés qu'un organisme d'évaluation de la conformité pourrait ne pas les utiliser, sous réserve de conditions spécifiques, en particulier l'approbation par l'autorité nationale de certification de cybersécurité.

(12) La certification des produits TIC au niveau AVA_VAN 4 ou 5 ne devrait être possible que dans des conditions spécifiques et lorsqu'une méthode d'évaluation spécifique est disponible. La méthode d'évaluation spécifique peut être inscrite dans des documents de référence pertinents pour le domaine technique, ou dans des profils de protection spécifiques adoptés en tant que documents de référence pertinents pour la catégorie de produits concernée. La certification à ces niveaux d'assurance ne devrait être possible que dans des cas exceptionnels et dûment justifiés, sous réserve de conditions spécifiques, en particulier l'approbation, notamment de la méthode d'évaluation applicable, par l'autorité nationale de certification de cybersécurité. Il pourrait exister des cas exceptionnels et dûment justifiés lorsque la législation de l'Union ou la législation nationale exige la certification d'un produit TIC au niveau AVA_VAN 4 ou 5. De même, dans des cas exceptionnels et dûment justifiés, les profils de protection pourraient être certifiés sans l'application des documents de référence pertinents, sous réserve de conditions spécifiques, en particulier l'approbation, notamment de la méthode d'évaluation applicable, par l'autorité nationale de certification de cybersécurité.

(13) Les marques et les étiquettes utilisées dans le cadre de l'EUCC visent à démontrer de manière visible la fiabilité du produit TIC certifié aux utilisateurs et à leur permettre de faire un choix éclairé lorsqu'ils achètent des produits TIC. L'utilisation des marques et des étiquettes devrait également être soumise aux règles et conditions énoncées dans la norme ISO/CEI 17065 et, le cas échéant, dans la norme ISO/CEI 17030 et ses lignes directrices applicables.

(14) Les organismes de certification devraient décider de la durée de validité des certificats en tenant compte du cycle de vie du produit TIC concerné. La durée de validité ne devrait pas dépasser cinq ans. Les autorités nationales de certification de cybersécurité devraient s'efforcer d'harmoniser la durée de validité dans l'Union.

(15) Lorsqu'un certificat EUCC existant voit son champ d'application réduit, il devrait être retiré et un nouveau certificat indiquant le nouveau champ d'application devrait être délivré pour que les utilisateurs soient tenus clairement informés du champ d'application et du niveau d'assurance du certificat d'un produit TIC donné.

(16) La certification des profils de protection est différente de celle des produits TIC car elle concerne un processus TIC. Sachant qu'un profil de protection couvre une catégorie de produits TIC, l'évaluation et la certification d'un profil de protection ne peuvent être effectuées sur la base d'un seul produit TIC. Étant donné qu'un profil de protection regroupe les exigences générales de sécurité concernant une catégorie de produits TIC, indépendamment de la manifestation du produit TIC par son vendeur, la période de validité d'un certificat EUCC pour un profil de protection devrait, en principe, couvrir cinq ans au minimum et pouvoir être étendue à la durée de vie du profil de protection.

(17) Un organisme d'évaluation de la conformité est un organisme qui effectue des opérations d'évaluation de la conformité, comme l'étalonnage, les essais, la certification et l'inspection. Afin de garantir une qualité élevée des services, le présent règlement précise que les opérations d'essai, d'une part, et les opérations de certification et d'inspection, d'autre part, devraient être effectuées par des entités opérant indépendamment les unes des autres, à savoir, respectivement, les centres d'évaluation de la sécurité des technologies de l'information («CESTI») et les organismes de certification. Ces deux types d'organismes d'évaluation de la conformité devraient être accrédités et, dans certains cas, autorisés.

(18) Un organisme de certification devrait être accrédité conformément à la norme ISO/CEI 17065 par l'organisme national d'accréditation pour les niveaux d'assurance «substantiel» et «élevé». En plus d'être accrédités conformément au règlement (UE) 2019/881, lu conjointement avec le règlement (CE) nº 765/2008, les organismes d'évaluation de la conformité devraient satisfaire à des exigences spécifiques afin de garantir leur compétence technique en vue de l'évaluation des exigences de cybersécurité au niveau d'assurance «élevé» du schéma EUCC, qui est confirmée par une «autorisation». Afin de soutenir le processus d'autorisation, il convient que des documents de référence pertinents soient élaborés, et qu'ils soient publiés par l'ENISA après approbation du groupe européen de certification de cybersécurité.

(19) La compétence technique d'un CESTI devrait être évaluée au moyen de l'accréditation des laboratoires d'essai prévue par la norme ISO/CEI 17025 et complétée par la norme ISO/CEI 23532-1 pour l'ensemble des activités d'évaluation qui sont pertinentes pour le niveau d'assurance et spécifiées dans la norme ISO/CEI 18045, conjointement avec la norme ISO/CEI 15408. L'organisme de certification ainsi que le CESTI devraient établir et tenir à jour un système approprié de gestion des compétences du personnel qui s'inspire de la norme ISO/CEI 19896-1 pour les éléments et les niveaux de compétence et pour l'appréciation des compétences. En ce qui concerne le niveau de connaissances, d'aptitudes, d'expérience et de formation, les exigences applicables aux évaluateurs devraient être inspirées de la norme ISO/CEI 19896-3. L'équivalence des dispositions et mesures prises pour combler les écarts avec ces systèmes de gestion des compétences devrait être démontrée, au regard des objectifs du système.

(20) Pour être autorisé, il y a lieu que le CESTI démontre sa capacité à déterminer l'absence de vulnérabilités connues, la mise en œuvre correcte et cohérente de fonctionnalités de sécurité de pointe pour la technologie spécifique concernée et la résistance du produit TIC ciblé par des attaques menées par des acteurs compétents. En outre, pour obtenir des autorisations dans le domaine technique des «cartes à puce et dispositifs similaires», il y a également lieu que le CESTI démontre les capacités techniques nécessaires aux activités d'évaluation et aux tâches connexes définies dans le document d'appui «Minimum ITSEF requirements for security evaluations of smart cards and similar devices» ([3]) (Exigences minimales du CESTI pour l'évaluation de la sécurité des cartes à puce et des dispositifs similaires, en anglais) dans le cadre des critères communs. Pour l'autorisation dans le domaine technique «dispositifs matériels avec boîtiers de sécurité», le CESTI devrait, en outre, démontrer les exigences techniques minimales nécessaires à la réalisation des activités d'évaluation et des tâches connexes relatives aux dispositifs matériels avec boîtiers de sécurité, conformément aux recommandations du GECC. Dans le cadre des exigences minimales, le CESTI devrait être en mesure de mener les différents types d'attaques décrits dans le document d'appui «Application of Attack Potential to Hardware Devices with Security Boxes» (Application du potentiel d'attaque aux dispositifs matériels avec boîtiers de sécurité, en anglais) dans le cadre des critères communs. Ces capacités englobent les connaissances et les compétences de l'évaluateur, ainsi que l'équipement et les méthodes d'évaluation nécessaires pour déterminer et évaluer les différents types d'attaques.

(21) L'autorité nationale de certification de cybersécurité devrait contrôler le respect, par les organismes de certification, le CESTI et les titulaires de certificats, de leurs obligations découlant du présent règlement et du règlement (UE) 2019/881. L'autorité nationale de certification de cybersécurité devrait utiliser toute source d'information appropriée à cette fin, y compris les informations reçues des participants au processus de certification ou obtenues au cours de ses propres enquêtes.

(22) Les organismes de certification devraient coopérer avec les autorités compétentes de surveillance du marché et tenir compte de toute information relative à la vulnérabilité qui pourrait concerner les produits TIC pour lesquels ils ont délivré des certificats. Les organismes de certification devraient contrôler les profils de protection qu'ils ont certifiés afin de déterminer si les exigences de sécurité définies pour une catégorie de produits TIC continuent de refléter les dernières évolutions en matière de cybermenace.

(23) À l'appui du contrôle de conformité, les autorités nationales de certification de cybersécurité devraient coopérer avec les autorités de surveillance du marché concernées, conformément à l'article 58 du règlement (UE) 2019/881 et au règlement (UE) 2019/1020 du Parlement européen et du Conseil ([4]). Les opérateurs économiques de l'Union sont tenus de partager des informations et de coopérer avec les autorités de surveillance du marché, conformément à l'article 4, paragraphe 3, du règlement (UE) 2019/1020.

([3]) Joint Interpretation Library: Minimum ITSEF Requirements for Security Evaluations of Smart cards and similar devices, version 2.1 de février 2020, disponible en anglais à l'adresse suivante: sogis.eu.

([4]) Règlement (UE) 2019/1020 du Parlement européen et du Conseil du 20 juin 2019 sur la surveillance du marché et la conformité des produits, et modifiant la directive 2004/42/CE et les règlements (CE) nº 765/2008 et (UE) nº 305/2011 (JO L 169 du 25.6.2019, p. 1).

(24) Les organismes de certification devraient contrôler si les titulaires de certificats respectent leurs obligations et contrôler la conformité de tous les certificats délivrés au titre de l'EUCC. Ce contrôle devrait garantir que tous les rapports d'évaluation fournis par un CESTI, les conclusions qui y sont tirées ainsi que les critères et méthodes d'évaluation sont appliqués de manière cohérente et correcte dans toutes les activités de certification.

(25) Lorsque des problèmes de non-conformité potentiels sont détectés pour un produit TIC certifié, il est important d'assurer une réaction proportionnelle. Les certificats pourront donc être suspendus. Cette suspension devrait entraîner certaines limitations concernant la promotion et l'utilisation du produit TIC en question, sans affecter la validité du certificat. La suspension devrait être notifiée aux acheteurs des produits TIC concernés par le titulaire du certificat européen, et aux autorités compétentes de surveillance du marché par l'autorité nationale de certification de cybersécurité. Pour informer le public, l'ENISA devrait publier des informations sur la suspension en question sur un site web prévu à cet effet.

(26) Le titulaire d'un certificat EUCC devrait mettre en œuvre les procédures de gestion des vulnérabilités nécessaires et veiller à ce que ces procédures soient intégrées dans son organisation. Lorsqu'il a connaissance d'une vulnérabilité potentielle, le titulaire du certificat EUCC devrait effectuer une analyse d'impact de la vulnérabilité. Si cette analyse confirme que la vulnérabilité peut être exploitée, le titulaire du certificat devrait envoyer un rapport d'évaluation à l'organisme de certification qui, à son tour, devrait en informer l'autorité nationale de certification de cybersécurité. Ce rapport devrait indiquer l'incidence de la vulnérabilité, les changements nécessaires ou les mesures correctives requises, ainsi que les éventuelles implications plus larges de la vulnérabilité et les solutions correctives pour d'autres produits. Le cas échéant, la norme EN ISO/CEI 29147 devrait compléter la procédure de divulgation de la vulnérabilité.

(27) Aux fins de la certification, les organismes d'évaluation de la conformité et les autorités nationales de certification de cybersécurité obtiennent des données confidentielles et sensibles et des secrets d'affaires, également liés à la propriété intellectuelle ou au contrôle de la conformité, qui nécessitent une protection adéquate. Ils devraient donc disposer des compétences et des connaissances techniques nécessaires et mettre en place des systèmes de protection des informations. Les exigences et conditions relatives à la protection des informations devraient être respectées tant pour l'accréditation que pour l'autorisation.

(28) L'ENISA devrait fournir la liste des profils de protection certifiés sur son site web de certification de cybersécurité et indiquer leur statut, conformément au règlement (UE) 2019/881.

(29) Le présent règlement fixe les conditions des accords de reconnaissance mutuelle avec les pays tiers. Ces accords de reconnaissance mutuelle peuvent être bilatéraux ou multilatéraux et devraient remplacer les accords similaires actuellement en place. Pour que la transition vers ces accords de reconnaissance mutuelle se fasse en douceur, les États membres peuvent continuer d'appliquer pendant un temps limité les accords de coopération existants conclus avec des pays tiers.

(30) Les organismes de certification délivrant des certificats EUCC au niveau d'assurance «élevé», ainsi que les CESTI associés, devraient faire l'objet d'évaluations par les pairs. L'objectif des évaluations par les pairs devrait consister à déterminer si les statuts et les procédures d'un organisme de certification évalué par les pairs restent conformes aux exigences du schéma EUCC. L'évaluation par les pairs est différente de l'examen par les pairs dont font l'objet les autorités nationales de certification de cybersécurité conformément à l'article 59 du règlement (UE) 2019/881. Les évaluations par les pairs devraient permettre de vérifier que les organismes de certification travaillent de manière harmonisée et produisent des certificats de même qualité. Elles devraient également permettre de recenser toute force ou faiblesse potentielle dans les performances des organismes de certification, notamment en vue de partager les meilleures pratiques. Étant donné qu'il existe différents types d'organisme de certification, il conviendrait d'autoriser différents types d'évaluation par les pairs. Dans des cas plus complexes, tels que celui des organismes de certification délivrant des certificats à différents niveaux AVA_VAN, plusieurs types d'évaluation par les pairs peuvent être utilisés, à condition que toutes les exigences soient respectées.

(31) Le groupe européen de certification de cybersécurité devrait jouer un rôle important dans le maintien du schéma. Pour ce faire, il devrait, entre autres, coopérer avec le secteur privé, créer des sous-groupes spécialisés et réaliser les travaux préparatoires et l'assistance demandés par la Commission. Le groupe européen de certification de cybersécurité joue un rôle important dans l'approbation des documents de référence. Lors de l'approbation et de l'adoption des documents de référence, il devrait être dûment tenu compte des éléments visés à l'article 54, paragraphe 1, point c), du règlement (UE) 2019/881. Les domaines techniques et les documents de référence

devraient être publiés à l'annexe I du présent règlement. Les profils de protection qui ont été adoptés en tant que documents de référence devraient être publiés à l'annexe II. Afin de garantir le caractère dynamique de ces annexes, la Commission peut les modifier, conformément à la procédure prévue à l'article 66, paragraphe 2, du règlement (UE) 2019/881, et en tenant compte de l'avis du groupe européen de certification de cybersécurité. L'annexe III contient des profils de protection recommandés qui, au moment de l'entrée en vigueur du présent règlement, ne sont pas des documents de référence. Ils devraient être publiés sur le site web de l'ENISA visé à l'article 50, paragraphe 1, du règlement (UE) 2019/881.

(32) Le présent règlement devrait commencer à s'appliquer douze mois après son entrée en vigueur. Les exigences du chapitre IV et de l'annexe V ne nécessitent pas de période de transition et devraient donc s'appliquer dès l'entrée en vigueur du présent règlement.

(33) Les mesures prévues au présent règlement sont conformes à l'avis du comité européen de certification de cybersécurité institué par l'article 66 du règlement (UE) 2019/881,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet et champ d'application

Le présent règlement établit le schéma européen de certification de cybersécurité fondé sur des critères communs (EUCC).

Le présent règlement s'applique à tous les produits des technologies de l'information et de la communication (TIC), y compris leur documentation, qui sont présentés pour certification dans le cadre de l'EUCC, ainsi qu'à tous les profils de protection qui sont présentés pour certification dans le cadre du processus TIC menant à la certification des produits TIC.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

1) «critères communs»: les critères communs pour l'évaluation de la sécurité des technologies de l'information, tels qu'ils figurent dans la norme ISO/CEI 15408;

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;

3) «cible d'évaluation»: un produit TIC ou une partie de celui-ci, ou un profil de protection dans le cadre d'un processus TIC, qui fait l'objet d'une évaluation de la cybersécurité en vue de recevoir la certification EUCC;

4) «cible de sécurité»: une déclaration d'exigences de sécurité dépendant de la mise en œuvre d'un produit TIC spécifique;

5) «profil de protection»: un processus TIC qui définit les exigences de sécurité relatives à une catégorie spécifique de produits TIC, répondant à des besoins de sécurité indépendants de la mise en œuvre, et qui peut être utilisé pour évaluer, aux fins de leur certification, les produits TIC relevant de cette catégorie spécifique;

6) «rapport technique d'évaluation»: un document produit par un CESTI pour présenter les conclusions, les verdicts et les justifications obtenus lors de l'évaluation d'un produit TIC ou d'un profil de protection réalisée conformément aux règles et aux obligations énoncées dans le présent règlement;

7) «CESTI»: un centre d'évaluation de la sécurité des technologies de l'information, qui est un organisme d'évaluation de la conformité, au sens de l'article 2, point 13), du règlement (CE) nº 765/2008, qui exécute des tâches d'évaluation;

8) «niveau AVA_VAN»: un niveau d'analyse de la vulnérabilité de l'assurance qui indique le degré des activités d'évaluation de la cybersécurité menées pour déterminer le niveau de résistance à l'exploitabilité potentielle des failles ou des faiblesses de la cible d'évaluation dans son environnement opérationnel, conformément aux critères communs;

9) «certificat EUCC»: un certificat de cybersécurité délivré au titre de l'EUCC pour des produits TIC, ou pour des profils de protection qui peuvent être utilisés exclusivement dans le cadre du processus de certification des produits TIC;

10) «produit composite»: un produit TIC évalué avec un autre produit TIC sous-jacent qui a déjà reçu un certificat EUCC et sur la fonctionnalité de sécurité duquel dépend le produit TIC composite;

11) «autorité nationale de certification de cybersécurité»: une autorité désignée par un État membre conformément à l'article 58, paragraphe 1, du règlement (UE) 2019/881;

12) «organisme de certification»: un organisme d'évaluation de la conformité, au sens de l'article 2, point 13), du règlement (CE) nº 765/2008, qui exerce des activités de certification;

13) «domaine technique»: un cadre technique commun lié à une technologie particulière pour la certification harmonisée comportant un ensemble d'exigences de sécurité caractéristiques;

14) «document de référence»: un document qui spécifie les méthodes, techniques et outils d'évaluation qui s'appliquent à la certification des produits TIC ou aux exigences de sécurité d'une catégorie générique de produits TIC, ou à toutes autres exigences nécessaires pour la certification, aux fins de l'harmonisation de l'évaluation, en particulier des domaines techniques ou des profils de protection;

15) «autorité de surveillance du marché»: une autorité définie à l'article 3, paragraphe 4, du règlement (UE) 2019/1020.

Article 3

Normes d'évaluation

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

a) les critères communs;

b) la méthode d'évaluation commune.

Article 4

Niveaux d'assurance

1. Les organismes de certification délivrent des certificats EUCC de niveau d'assurance «substantiel» ou «élevé».

2. Les certificats EUCC de niveau d'assurance «substantiel» couvrent les niveaux AVA_VAN 1 ou 2.

3. Les certificats EUCC de niveau d'assurance «élevé» couvrent les niveaux AVA_VAN 3, 4 ou 5.

4. Le niveau d'assurance confirmé dans un certificat EUCC fait la distinction entre l'utilisation conforme et l'utilisation renforcée des composants d'assurance tels que spécifiés dans les critères communs conformément à l'annexe VIII.

5. Les organismes d'évaluation de la conformité appliquent les composants d'assurance dont dépend le niveau AVA_VAN sélectionné en se conformant aux normes visées à l'article 3.

Article 5

Méthodes de certification des produits TIC

1. La certification d'un produit TIC est effectuée par rapport à la cible de sécurité du produit:

a) telle qu'elle est définie par le demandeur; ou

b) en intégrant 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. Les profils de protection sont certifiés à la seule fin de la certification des produits TIC relevant de la catégorie spécifique de produits TIC couverte par le profil de protection.

Article 6

Autoévaluation de la conformité

L'autoévaluation de la conformité au sens de l'article 53 du règlement (UE) 2019/881 n'est pas autorisée.

CHAPITRE II

CERTIFICATION DES PRODUITS TIC

SECTION I

Normes et exigences spécifiques pour l'évaluation

Article 7

Critères et méthodes d'évaluation des produits TIC

1. Un produit TIC présenté pour certification est, au minimum, évalué au regard des éléments ci-dessous:

a) les éléments applicables des normes visées à l'article 3;

b) les catégories d'exigences en matière d'assurance de sécurité pour l'évaluation de la vulnérabilité et les essais fonctionnels indépendants, telles que définies dans les normes d'évaluation visées à l'article 3;

c) le niveau de risque associé à l'utilisation prévue des produits TIC concernés conformément à l'article 52 du règlement (UE) 2019/881 et leurs fonctions de sécurité qui soutiennent les objectifs de sécurité énoncés à l'article 51 du règlement (UE) 2019/881;

d) les documents de référence applicables énumérés à l'annexe I; et

e) les profils de protection certifiés applicables énumérés à l'annexe II.

2. Dans des cas exceptionnels et dûment justifiés, un organisme d'évaluation de la conformité peut demander à ne pas appliquer le document de référence pertinent. Dans ce cas, l'organisme d'évaluation de la conformité en informe l'autorité nationale de certification de cybersécurité en motivant dûment sa demande. L'autorité nationale de certification de cybersécurité évalue le motif de l'exception demandée et, lorsque cela se justifie, l'approuve. Dans l'attente de la décision de

l'autorité nationale de certification de cybersécurité, l'organisme d'évaluation de la conformité ne délivre aucun certificat. L'autorité nationale de certification de cybersécurité notifie, sans retard injustifié, l'exception approuvée au groupe européen de certification de cybersécurité, qui peut émettre un avis. L'autorité nationale de certification de cybersécurité tient le plus grand compte de l'avis du groupe européen de certification de cybersécurité.

3. La certification des produits TIC au niveau AVA_VAN 4 ou 5 n'est possible que dans les scénarios suivants:

a) lorsque le produit TIC relève d'un des domaines techniques énumérés à l'annexe I, il est évalué conformément aux documents de référence applicables de ces domaines techniques;

b) lorsque le produit TIC relève d'une catégorie de produits TIC couverts par un profil de protection certifié comprenant les niveaux AVA_VAN 4 ou 5 et qui a été répertorié en tant que profil de protection de référence à l'annexe II, il est évalué conformément à la méthode d'évaluation spécifiée pour ce profil de protection;

c) lorsque les points a) et b) du présent paragraphe ne sont pas applicables et que l'inclusion d'un domaine technique dans l'annexe I ou d'un profil de protection certifié dans l'annexe II est improbable dans un avenir prévisible, et uniquement dans des cas exceptionnels et dûment justifiés, sous réserve des conditions énoncées au paragraphe 4.

4. Lorsqu'un organisme d'évaluation de la conformité considère qu'il se trouve dans un cas exceptionnel et dûment justifié visé au paragraphe 3, point c), il notifie la certification envisagée à l'autorité nationale de certification de cybersécurité en lui en expliquant les raisons et en lui proposant une méthode d'évaluation. L'autorité nationale de certification de cybersécurité évalue le motif de l'exception demandée et, lorsque cela se justifie, approuve ou modifie la méthode d'évaluation à appliquer par l'organisme d'évaluation de la conformité. Dans l'attente de la décision de l'autorité nationale de certification de cybersécurité, l'organisme d'évaluation de la conformité ne délivre aucun certificat. L'autorité nationale de certification de cybersécurité notifie, sans retard injustifié, la certification envisagée au groupe européen de certification de cybersécurité, qui peut émettre un avis. L'autorité nationale de certification de cybersécurité tient le plus grand compte de l'avis du groupe européen de certification de cybersécurité.

5. Dans le cas d'un produit TIC faisant l'objet d'une évaluation de produit composite conformément aux documents de référence pertinents, le CESTI qui a procédé à l'évaluation du produit TIC sous-jacent partage les informations pertinentes avec le CESTI qui procède à l'évaluation du produit TIC composite.

SECTION II

Délivrance, renouvellement et retrait des certificats EUCC

Article 8

Informations nécessaires pour la certification

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.

2. Les informations visées au paragraphe 1 comprennent tous les éléments de preuve pertinents conformément aux sections relatives aux «Éléments d'action du développeur» dans le format approprié, comme indiqué dans les sections relatives au «Contenu et présentation des éléments de preuve» des critères communs et de la méthode d'évaluation commune pour le niveau d'assurance choisi et les exigences d'assurance de sécurité associées. Les éléments de preuve comprennent, si nécessaire, des détails sur le produit TIC et son code source conformément au présent règlement, sous réserve de garanties contre toute divulgation non autorisée.

3. Les candidats à la certification peuvent fournir à l'organisme de certification et au CESTI des résultats d'évaluation appropriés provenant d'une certification antérieure en vertu:

a) du présent règlement;

b) d'un autre schéma européen de certification de cybersécurité adopté conformément à l'article 49 du règlement (UE) 2019/881;

c) d'un schéma national visé à l'article 49 du présent règlement.

4. Lorsque les résultats de l'évaluation sont pertinents pour ses tâches, le CESTI peut réutiliser les résultats d'évaluation fournis à condition que ces preuves soient conformes aux exigences applicables et que leur authenticité soit confirmée.

5. Lorsque l'organisme de certification autorise la soumission du produit à un processus de certification de produit composite, le candidat à la certification met à la disposition de l'organisme de certification et du CESTI tous les éléments nécessaires, le cas échéant, conformément au document de référence.

6. Le candidat à la certification fournit également à l'organisme de certification et au CESTI les informations suivantes:

a) le lien vers son site web contenant les informations supplémentaires en matière de cybersécurité visées à l'article 55 du règlement (UE) 2019/881;

b) une description des procédures de gestion et de divulgation des vulnérabilités du demandeur.

7. Toute la documentation pertinente visée au présent article est conservée par l'organisme de certification, par le CESTI et par le demandeur pendant une période de cinq ans après l'expiration du certificat.

Article 9

Conditions de délivrance d'un certificat EUCC

1. Les organismes de certification délivrent un certificat EUCC lorsque toutes les conditions suivantes sont remplies:

a) la catégorie de produit TIC relève du champ d'application de l'accréditation, et le cas échéant de l'autorisation, de l'organisme de certification et du CESTI concernés par la certification;

b) le candidat à la certification a signé une déclaration dans laquelle il s'engage à honorer tous les engagements énumérés au paragraphe 2;

c) le CESTI a conclu l'évaluation sans objection conformément aux normes, critères et méthodes d'évaluation visés aux articles 3 et 7;

d) l'organisme de certification a conclu l'examen des résultats de l'évaluation sans objection;

e) l'organisme de certification a vérifié que les rapports techniques d'évaluation fournis par le CESTI sont conformes aux preuves fournies et que les normes, critères et méthodes d'évaluation visés aux articles 3 et 7 ont été appliqués correctement.

2. Le candidat à la certification prend les engagements suivants:

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;

b) ne pas promouvoir le produit TIC comme étant certifié EUCC avant que le certificat EUCC ne soit délivré;

c) promouvoir le produit TIC comme étant certifié uniquement en ce qui concerne le champ d'application défini dans le certificat EUCC;

d) cesser immédiatement de promouvoir le produit TIC comme étant certifié en cas de suspension, de retrait ou d'expiration du certificat EUCC;

e) s'assurer que les produits TIC vendus comme étant certifiés EUCC sont strictement identiques au produit TIC faisant l'objet de la certification;

f) respecter les règles d'utilisation de la marque et de l'étiquette établies pour le certificat EUCC conformément à l'article 11.

3. Dans le cas d'un produit TIC faisant l'objet d'une certification de produit composite conformément aux documents de référence pertinents, l'organisme de certification qui a procédé à la certification du produit TIC sous-jacent partage les informations pertinentes avec l'organisme de certification qui procède à la certification du produit TIC composite.

Article 10

Contenu et format d'un certificat EUCC

1. Le certificat EUCC comprend au moins les informations mentionnées à l'annexe VII.

2. La portée et les limites du produit TIC certifié sont précisées sans ambiguïté dans le certificat EUCC ou dans le rapport de certification, en indiquant si l'ensemble du produit TIC a été certifié ou seulement des parties de celui-ci.

3. L'organisme de certification fournit le certificat EUCC au demandeur au moins sous forme électronique.

4. L'organisme de certification établit un rapport de certification conformément à l'annexe V pour chaque certificat EUCC qu'il délivre. Le rapport de certification se fonde sur le rapport technique d'évaluation émis par le CESTI. Le rapport technique d'évaluation et le rapport de certification indiquent les critères et méthodes d'évaluation spécifiques visés à l'article 7 utilisés pour l'évaluation.

5. L'organisme de certification fournit à l'autorité nationale de certification de cybersécurité et à l'ENISA chaque certificat EUCC et chaque rapport de certification sous forme électronique.

Article 11

Marque et étiquette

1. Le titulaire d'un certificat peut apposer une marque et une étiquette sur un produit TIC certifié. La marque et l'étiquette indiquent que le produit TIC a été certifié conformément au présent règlement. La marque et l'étiquette sont apposées conformément au présent article et à l'annexe IX.

2. La marque et l'étiquette sont apposées de manière visible, lisible et indélébile sur le produit TIC certifié ou sur sa plaque signalétique. Si cela est impossible ou n'est pas justifié en raison de la nature du produit, elles sont apposées sur l'emballage et sur les documents d'accompagnement. Lorsque le produit TIC certifié est livré sous la forme d'un logiciel, la marque et l'étiquette apparaissent de manière visible, lisible et indélébile dans la documentation qui l'accompagne, ou cette documentation est rendue facilement et directement accessible aux utilisateurs au moyen d'un site web.

3. La marque et l'étiquette figurent à l'annexe IX et contiennent:

a) le niveau d'assurance et le niveau AVA_VAN du produit TIC certifié;

b) l'identifiant unique du certificat, comprenant:

   1) le nom du schéma;

   2) le nom de l'organisme de certification qui a délivré le certificat, et le numéro de référence de son accréditation;

   3) l'année et le mois de délivrance;

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

4. La marque et l'étiquette sont accompagnées d'un code QR avec un lien vers un site web contenant au moins:

a) les informations sur la validité du certificat;

b) les informations nécessaires relatives à la certification, telles qu'elles figurent aux annexes V et VII;

c) les informations que le titulaire du certificat est tenu de mettre à la disposition du public conformément à l'article 55 du règlement (UE) 2019/881; et

d) le cas échéant, les informations historiques relatives aux certifications spécifiques du produit TIC afin de permettre la traçabilité.

Article 12

Durée de validité d'un certificat EUCC

1. L'organisme de certification fixe la durée de validité de chaque certificat EUCC délivré en tenant compte des caractéristiques du produit TIC certifié.

2. La durée maximale de validité d'un certificat EUCC est de cinq ans.

3. Par dérogation au paragraphe 2, cette durée peut dépasser cinq ans, sous réserve de l'approbation préalable de l'autorité nationale de certification de cybersécurité. L'autorité nationale de certification de cybersécurité notifie sans délai au groupe européen de certification de cybersécurité l'approbation accordée.

Article 13

Réexamen d'un certificat EUCC

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 produit TIC. 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 produit TIC certifié.

2. Sur la base des résultats du réexamen et, le cas échéant, de la réévaluation, l'organisme de certification:

a) confirme le certificat EUCC;

b) retire le certificat EUCC conformément à l'article 14;

c) retire le certificat EUCC conformément à l'article 14 et délivre un nouveau certificat EUCC avec un champ d'application identique et une durée de validité prolongée; ou

d) retire le certificat EUCC conformément à l'article 14 et délivre un nouveau certificat EUCC avec un champ d'application différent.

3. L'organisme de certification peut décider de suspendre, sans retard injustifié, le certificat EUCC conformément à l'article 30, en attendant que le titulaire du certificat EUCC prenne des mesures correctives.

Article 14

Retrait d'un certificat EUCC

1. Sans préjudice de l'article 58, paragraphe 8, point e), du règlement (UE) 2019/881, un certificat EUCC est retiré par l'organisme de certification qui l'a délivré.

2. L'organisme de certification visé au paragraphe 1 notifie le retrait du certificat à l'autorité nationale de certification de cybersécurité. Il notifie également ce retrait à l'ENISA afin de faciliter l'exécution de sa mission au titre de l'article 50 du règlement (UE) 2019/881. L'autorité nationale de certification de cybersécurité en informe les autres autorités de surveillance du marché concernées.

3. Le titulaire d'un certificat EUCC peut demander le retrait du certificat.

CHAPITRE III

CERTIFICATION DES PROFILS DE PROTECTION

SECTION I

Normes et exigences spécifiques pour l'évaluation

Article 15

Critères et méthodes d'évaluation

1. Un profil de protection est évalué, au minimum, par rapport aux éléments ci-dessous:

a) les éléments applicables des normes visées à l'article 3;

b) le niveau de risque associé à l'utilisation prévue des produits TIC concernés conformément à l'article 52 du règlement (UE) 2019/881 et leurs fonctions de sécurité qui soutiennent les objectifs de sécurité énoncés à l'article 51 de ce même règlement; et

c) les documents de référence applicables énumérés à l'annexe I. Un profil de protection couvert par un domaine technique est certifié par rapport aux exigences définies dans ce domaine technique.

2. Dans des cas exceptionnels et dûment justifiés, un organisme d'évaluation de la conformité peut certifier un profil de protection sans appliquer les documents de référence pertinents. Dans ce cas, il en informe l'autorité nationale de certification de cybersécurité compétente en fournissant une justification pour la certification sans application des documents de référence pertinents envisagée et en proposant une méthode d'évaluation. L'autorité nationale de certification de cybersécurité évalue cette justification et, lorsque celle-ci est fondée, approuve la non-application des documents de référence pertinents, et approuve ou modifie, le cas échéant, la méthode d'évaluation à appliquer par l'organisme d'évaluation de la conformité. Dans l'attente de la décision de l'autorité nationale de certification de cybersécurité, l'organisme d'évaluation de la conformité ne délivre aucun certificat pour le profil de protection. L'autorité nationale de certification de cybersécurité notifie, sans retard injustifié, l'autorisation de ne pas appliquer les documents de référence pertinents au groupe européen de certification de cybersécurité, qui peut émettre un avis. L'autorité nationale de certification de cybersécurité tient le plus grand compte de l'avis du groupe européen de certification de cybersécurité.

SECTION II

Délivrance, renouvellement et retrait des certificats EUCC pour les profils de protection

Article 16

Informations nécessaires pour la certification 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. L'article 8, paragraphes 2, 3, 4 et 7, s'applique mutatis mutandis.

Article 17

Délivrance de certificats EUCC pour les profils de protection

1. Le candidat à la certification fournit à l'organisme de certification et au CESTI toutes les informations nécessaires, complètes et correctes.

2. Les articles 9 et 10 s'appliquent mutatis mutandis.

3. Le CESTI évalue si un profil de protection est complet, cohérent, solide techniquement et efficace pour l'utilisation prévue et les objectifs de sécurité de la catégorie de produits TIC couverte par ce profil de protection.

4. Un profil de protection est certifié uniquement par:

a) une autorité nationale de certification de cybersécurité ou un autre organisme public accrédité en tant qu'organisme de certification; ou

b) un organisme de certification, après approbation préalable de l'autorité nationale de certification de cybersécurité pour chaque profil de protection individuel.

Article 18

Durée de validité d'un certificat EUCC pour les profils de protection

1. L'organisme de certification fixe une durée de validité pour chaque certificat EUCC.

2. La durée de validité peut être égale à la durée de vie du profil de protection concerné.

Article 19

Réexamen du certificat EUCC d'un profil de protection

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 aux conditions prévues à l'article 15. 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.

2. Sur la base des résultats du réexamen et, le cas échéant, de la réévaluation, l'organisme de certification prend l'une des mesures suivantes:

a) confirmer le certificat EUCC;

b) retirer le certificat EUCC conformément à l'article 20;

c) retire le certificat EUCC conformément à l'article 20 et délivre un nouveau certificat EUCC avec un champ d'application identique et une durée de validité prolongée;

d) retire le certificat EUCC conformément à l'article 20 et délivre un nouveau certificat EUCC avec un champ d'application différent.

Article 20

Retrait du certificat EUCC d'un profil de protection

1. Sans préjudice de l'article 58, paragraphe 8, point e), du règlement (UE) 2019/881, un certificat EUCC de profil de protection peut être retiré par l'organisme de certification qui a délivré ce certificat. L'article 14 s'applique mutatis mutandis.

2. Un certificat pour un profil de protection délivré conformément à l'article 17, paragraphe 4, point b), est retiré par l'autorité nationale de certification de cybersécurité qui l'a approuvé.

CHAPITRE IV

ORGANISMES D'ÉVALUATION DE LA CONFORMITÉ

Article 21

Exigences supplémentaires ou spécifiques pour un organisme de certification

1. Un organisme de certification est autorisé par l'autorité nationale de certification de cybersécurité à délivrer des certificats EUCC de niveau d'assurance «élevé» lorsque cet organisme démontre, en plus de répondre aux exigences énoncées à l'article 60, paragraphe 1, et à l'annexe du règlement (UE) 2019/881 concernant l'accréditation des organismes d'évaluation de la conformité:

a) qu'il a l'expertise et les compétences requises pour la décision de certification au niveau d'assurance «élevé»;

b) qu'il mène ses activités de certification en coopération avec un CESTI autorisé conformément à l'article 22; et

c) qu'il a les compétences requises et a mis en place les mesures techniques et opérationnelles appropriées pour protéger efficacement les informations confidentielles et sensibles pour le niveau d'assurance «élevé», en plus des exigences énoncées à l'article 43.

2. L'autorité nationale de certification de cybersécurité évalue si un organisme de certification respecte toutes les exigences énoncées au paragraphe 1. Cette évaluation comprend au moins des entretiens structurés et un examen d'au moins une certification pilote réalisés par l'organisme de certification conformément au présent règlement.

Dans son évaluation, l'autorité nationale de certification de cybersécurité peut réutiliser tout élément de preuve approprié provenant d'une autorisation préalable ou d'activités similaires octroyées en vertu:

a) du présent règlement;

b) d'un autre schéma européen de certification de cybersécurité adopté conformément à l'article 49 du règlement (UE) 2019/881;

c) d'un schéma national visé à l'article 49 du présent règlement.

3. L'autorité nationale de certification de cybersécurité établit un rapport d'autorisation qui fait l'objet d'un examen par les pairs conformément à l'article 59, paragraphe 3, point d), du règlement (UE) 2019/881.

4. L'autorité nationale de certification de cybersécurité précise les catégories de produit TIC et les profils de protection auxquels l'autorisation s'étend. L'autorisation est valable pour une période n'excédant pas la durée de validité de l'accréditation. Elle peut être renouvelée sur demande, à condition que l'organisme de certification continue de respecter les exigences énoncées dans le présent article. Aucune évaluation pilote n'est requise pour le renouvellement de l'autorisation.

5. L'autorité nationale de certification de cybersécurité retire l'autorisation de l'organisme de certification lorsque celui-ci ne remplit plus les conditions énoncées dans le présent article. En cas de retrait de l'autorisation, l'organisme de certification cesse immédiatement de se présenter comme un organisme de certification autorisé.

Article 22

Exigences supplémentaires ou spécifiques applicables à un CESTI

1. Un CESTI est autorisé par l'autorité nationale de certification de cybersécurité à procéder à l'évaluation de produits TIC qui font l'objet d'une certification au niveau d'assurance «élevé» lorsqu'il démontre, en plus de répondre aux exigences énoncées à l'article 60, paragraphe 1, et à l'annexe du règlement (UE) 2019/881 concernant l'accréditation des organismes d'évaluation de la conformité, qu'il respecte l'ensemble des conditions suivantes:

a) il a l'expertise nécessaire pour effectuer les opérations d'évaluation visant à déterminer la résistance aux cyberattaques de pointe perpétrées par des acteurs disposant de compétences et de ressources importantes;

b) pour les domaines techniques et les profils de protection qui font partie du processus TIC de ces produits TIC, il a:

1) l'expertise nécessaire pour réaliser les opérations d'évaluation spécifiques nécessaires pour déterminer méthodiquement la résistance d'une cible d'évaluation face à des attaquants compétents dans son environnement opérationnel, en cas d'attaque au potentiel «modéré» ou «élevé», comme indiqué dans les normes visées à l'article 3;

2) les compétences techniques spécifiées dans les documents de référence énumérés à l'annexe I;

c) il a les compétences requises et a mis en place les mesures techniques et opérationnelles appropriées pour protéger efficacement les informations confidentielles et sensibles pour le niveau d'assurance «élevé», en plus des exigences énoncées à l'article 43.

2. L'autorité nationale de certification de cybersécurité évalue si un CESTI remplit toutes les exigences énoncées au paragraphe 1. Cette évaluation comprend au moins des entretiens structurés et un examen d'au moins une évaluation pilote réalisée par le CESTI conformément au présent règlement.

3. Dans son évaluation, l'autorité nationale de certification de cybersécurité peut réutiliser tout élément de preuve approprié provenant d'une autorisation préalable ou d'activités similaires octroyées en vertu:

a) du présent règlement;

b) d'un autre schéma européen de certification de cybersécurité adopté conformément à l'article 49 du règlement (UE) 2019/881;

c) d'un schéma national visé à l'article 49 du présent règlement.

4. L'autorité nationale de certification de cybersécurité établit un rapport d'autorisation qui fait l'objet d'un examen par les pairs conformément à l'article 59, paragraphe 3, point d), du règlement (UE) 2019/881.

5. L'autorité nationale de certification de cybersécurité précise les catégories de produit TIC et les profils de protection auxquels l'autorisation s'étend. L'autorisation est valable pour une période n'excédant pas la durée de validité de l'accréditation. Elle peut être renouvelée sur demande, à condition que le CESTI continue de respecter les exigences énoncées dans le présent article. Aucune évaluation pilote ne devrait être requise pour le renouvellement de l'autorisation.

6. L'autorité nationale de certification de cybersécurité retire l'autorisation du CESTI si ce dernier ne remplit plus les conditions énoncées dans le présent article. Dès le retrait de l'autorisation, le CESTI cesse de se présenter comme un CESTI autorisé.

Article 23

Notification des organismes de certification

1. L'autorité nationale de certification de cybersécurité notifie à la Commission les organismes de certification présents sur son territoire et dont l'accréditation confirme qu'ils sont compétents pour délivrer des certificats de niveau d'assurance «substantiel».

2. L'autorité nationale de certification de cybersécurité notifie à la Commission les organismes de certification présents sur son territoire et dont l'accréditation et la décision d'autorisation confirment qu'ils sont compétents pour délivrer des certificats de niveau d'assurance «élevé».

3. Lorsqu'elle notifie un organisme de certification à la Commission, l'autorité nationale de certification de cybersécurité fournit au moins les informations suivantes:

a) le ou les niveaux d'assurance pour lesquels l'organisme de certification est compétent en matière de délivrance de certificats EUCC;

b) les informations suivantes relatives à l'accréditation:

1) la date de l'accréditation;

2) le nom et l'adresse de l'organisme de certification;

3) les pays d'enregistrement de l'organisme de certification;

4) le numéro de référence de l'accréditation;

5) le champ et la durée de validité de l'accréditation;

6) l'adresse, l'emplacement et le lien vers le site web de l'organisme national d'accréditation; et

c) les informations suivantes relatives à l'autorisation pour le niveau «élevé»:

1) la date de l'autorisation;

2) le numéro de référence de l'autorisation;

3) la durée de validité de l'autorisation;

4) le champ de l'autorisation, y compris le niveau AVA_VAN le plus élevé et, le cas échéant, le domaine technique couvert.

4. L'autorité nationale de certification de cybersécurité envoie à l'ENISA une copie de la notification visée aux paragraphes 1 et 2 aux fins de la publication, sur le site web consacré à la certification de cybersécurité, d'informations précises concernant l'éligibilité des organismes de certification.

5. L'autorité nationale de certification de cybersécurité examine sans retard excessif toute information concernant un changement de statut de l'accréditation fournie par l'organisme national d'accréditation. En cas de retrait de l'accréditation ou de l'autorisation, l'autorité nationale de certification de cybersécurité en informe la Commission et peut lui soumettre une demande conformément à l'article 61, paragraphe 4, du règlement (UE) 2019/881.

Article 24

Notification des CESTI

Les obligations de notification incombant aux autorités nationales de certification de cybersécurité, énoncées à l'article 23, s'appliquent également aux CESTI. La notification inclut l'adresse du CESTI, l'accréditation en cours de validité et, le cas échéant, l'autorisation en cours de validité de ce CESTI.

CHAPITRE V

CONTRÔLE, NON-CONFORMITÉ ET NON-RESPECT DES RÈGLES

SECTION I

Contrôle de conformité

Article 25

Activités de contrôle menées par l'autorité nationale de certification de cybersécurité

1. Sans préjudice de l'article 58, paragraphe 7, du règlement (UE) 2019/881, l'autorité nationale de certification de cybersécurité contrôle:

a) si l'organisme de certification et le CESTI respectent les obligations qui leur incombent en vertu du présent règlement et du règlement (UE) 2019/881;

b) les titulaires d'un certificat EUCC respectent les obligations qui leur incombent en vertu du présent règlement et du règlement (UE) 2019/881;

c) si les produits TIC certifiés respectent les exigences énoncées dans le schéma EUCC;

d) si l'assurance indiquée dans le certificat EUCC concernant l'évolution du paysage des menaces est respectée.

2. L'autorité nationale de certification de cybersécurité exerce ses activités de contrôle sur la base notamment:

a) des informations provenant des organismes de certification, des organismes nationaux d'accréditation et des autorités compétentes de surveillance du marché;

b) des informations issues de ses propres audits et enquêtes ou de ceux d'une autre autorité;

c) de l'échantillonnage effectué conformément au paragraphe 3;

d) des plaintes reçues.

3. L'autorité nationale de certification de cybersécurité, en coopération avec d'autres autorités de surveillance du marché, prélève chaque année un échantillon d'au moins 4 % des certificats EUCC, tel que déterminé par une évaluation des risques. Sur demande et au nom de l'autorité nationale de certification de cybersécurité compétente, les organismes de certification et, si nécessaire, le CESTI aident cette autorité à contrôler la conformité.

4. L'autorité nationale de certification de cybersécurité sélectionne l'échantillon de produits TIC certifiés à contrôler sur la base de critères objectifs, y compris:

a) la catégorie de produits;

b) les niveaux d'assurance des produits;

c) le titulaire d'un certificat;

d) l'organisme de certification et, le cas échéant, le CESTI sous-traitant;

e) toute autre information portée à la connaissance de l'autorité.

5. L'autorité nationale de certification de cybersécurité informe les titulaires du certificat EUCC des produits TIC sélectionnés et des critères de sélection.

6. L'organisme de certification qui a certifié le produit TIC échantillonné procède, à la demande de l'autorité nationale de certification de cybersécurité, avec l'aide du CESTI respectif, à un examen complémentaire conformément à la procédure prévue à l'annexe IV, section IV.2, et informe l'autorité nationale de certification de cybersécurité des résultats.

7. Lorsque l'autorité nationale de certification de cybersécurité a des raisons suffisantes de croire qu'un produit TIC certifié n'est plus conforme au présent règlement ou au règlement (UE) 2019/881, elle peut mener des enquêtes ou faire usage de tout autre pouvoir de contrôle énoncé à l'article 58, paragraphe 8, du règlement (UE) 2019/881.

8. L'autorité nationale de certification de cybersécurité informe l'organisme de certification et le CESTI concerné des enquêtes en cours concernant les produits TIC sélectionnés.

9. Lorsque l'autorité nationale de certification de cybersécurité constate qu'une enquête en cours concerne des produits TIC certifiés par des organismes de certification établis dans d'autres États membres, elle en informe les autorités nationales de certification de cybersécurité des États membres concernés afin qu'elles collaborent aux enquêtes, le cas échéant. Ladite autorité nationale de certification de cybersécurité informe également le groupe européen de certification de cybersécurité des enquêtes transfrontières et de leurs résultats.

Article 26

Activités de contrôle menées par l'organisme de certification

1. L'organisme de certification contrôle:

a) le respect, par les titulaires d'un certificat, de leurs obligations au titre du présent règlement et du règlement (UE) 2019/881 à l'égard du certificat EUCC qui a été délivré par l'organisme de certification;

b) la conformité des produits TIC qu'il a certifiés avec les exigences de sécurité correspondantes;

c) l'assurance indiquée dans les profils de protection certifiés.

2. L'organisme de certification fonde ses activités de contrôle sur:

a) les informations fournies sur la base des engagements du candidat à la certification visés à l'article 9, paragraphe 2;

b) les informations provenant des activités des autres autorités compétentes de surveillance du marché;

c) les plaintes reçues;

d) les informations relatives aux vulnérabilités susceptibles d'avoir une incidence sur les produits TIC qu'il a certifiés.

3. L'autorité nationale de certification de cybersécurité peut fixer des règles afin d'établir un dialogue régulier entre les organismes de certification et les titulaires de certificats EUCC pour vérifier le respect des engagements pris en vertu de l'article 9, paragraphe 2 et pour rendre compte dudit respect, sans préjudice des activités liées à d'autres autorités de surveillance du marché compétentes.

Article 27

Activités de contrôle menées par le titulaire du certificat

1. Le titulaire d'un certificat EUCC effectue les tâches suivantes pour contrôler la conformité du produit TIC certifié avec les exigences de sécurité correspondantes:

a) surveiller les informations relatives aux vulnérabilités concernant le produit TIC certifié, y compris les dépendances connues, par ses propres moyens mais aussi en tenant compte:

   1) d'une publication ou d'une soumission contenant des informations sur les vulnérabilités de la part d'un utilisateur ou d'un chercheur dans le domaine de la sécurité tel que visé à l'article 55, paragraphe 1, point c), du règlement (UE) 2019/881;

   2) des informations communiquées par toute autre source;

b) contrôler l'assurance indiquée dans le certificat EUCC.

2. Le titulaire d'un certificat EUCC travaille en coopération avec l'organisme de certification, le CESTI et, le cas échéant, l'autorité nationale de certification de cybersécurité pour soutenir leurs activités de contrôle.

SECTION II

Conformité et respect des règles

Article 28

Conséquences de la non-conformité d'un produit TIC ou d'un profil de protection certifié

1. Lorsqu'un produit TIC ou un profil de protection certifié n'est pas conforme aux exigences énoncées dans le présent règlement et dans le règlement (UE) 2019/881, l'organisme de certification informe le titulaire du certificat EUCC de la non-conformité constatée et lui demande de prendre des mesures correctives.

2. Lorsqu'un cas de non-conformité avec les dispositions du présent règlement pourrait affecter la conformité avec une autre législation pertinente de l'Union prévoyant la possibilité de démontrer la présomption de conformité avec les exigences de l'acte juridique en question au moyen du certificat EUCC, l'organisme de certification en informe l'autorité nationale de certification de cybersécurité dans les meilleurs délais. L'autorité nationale de certification de cybersécurité notifie immédiatement le cas de non-conformité détecté à l'autorité de surveillance du marché responsable de l'autre acte législatif pertinent de l'Union.

3. Dès réception des informations visées au paragraphe 1, le titulaire du certificat EUCC propose à l'organisme de certification, dans le délai fixé par ce dernier, qui ne peut dépasser 30 jours, les mesures correctives nécessaires pour remédier à la non-conformité.

4. L'organisme de certification peut suspendre, sans retard injustifié, le certificat EUCC conformément à l'article 30 en cas d'urgence ou si le titulaire du certificat EUCC ne coopère pas dûment avec l'organisme de certification.

5. L'organisme de certification procède à un réexamen conformément aux articles 13 et 19, afin d'évaluer si la mesure corrective permet de remédier à la non-conformité.

6. Si le titulaire du certificat EUCC ne propose pas de mesure corrective appropriée au cours de la période visée au paragraphe 3, le certificat est suspendu conformément à l'article 30 ou retiré conformément aux articles 14 ou 20.

7. Le présent article ne s'applique pas aux cas de vulnérabilités concernant un produit TIC certifié, traités au chapitre VI.

Article 29

Conséquences de la non-conformité du titulaire du certificat

1. Lorsque l'organisme de certification constate que:

a) le titulaire du certificat EUCC ou le candidat à la certification ne respecte pas ses engagements et obligations définis à l'article 9, paragraphe 2, à l'article 17, paragraphe 2, et aux articles 27 et 41; ou

b) le titulaire du certificat EUCC ne respecte pas l'article 56, paragraphe 8, du règlement (UE) 2019/881 ou le chapitre VI du présent règlement;

il fixe un délai ne dépassant pas 30 jours dans lequel le titulaire du certificat EUCC prend des mesures correctives.

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

3. Le non-respect continu ou récurrent par le titulaire du certificat EUCC des obligations visées au paragraphe 1 déclenche le retrait du certificat EUCC conformément à l'article 14 ou 20.

4. L'organisme de certification informe l'autorité nationale de certification de cybersécurité des constatations visées au paragraphe 1. Lorsque le cas de non-conformité affecte la conformité avec d'autres législations pertinentes de l'Union, l'autorité nationale de certification de cybersécurité informe immédiatement du cas de non-conformité constaté l'autorité de surveillance du marché responsable de ces autres législations pertinentes de l'Union.

Article 30

Suspension du certificat EUCC

1. Lorsque le présent règlement fait référence à la suspension d'un certificat EUCC, l'organisme de certification suspend le certificat EUCC concerné pendant une période adaptée aux circonstances ayant déclenché la suspension, qui ne dépasse pas 42 jours. La période de suspension commence le jour suivant celui de la décision de l'organisme de certification. La suspension n'affecte pas la validité du certificat.

2. L'organisme de certification notifie la suspension au titulaire du certificat et à l'autorité nationale de certification de cybersécurité dans les meilleurs délais, en indiquant les motifs de la suspension, les mesures demandées et la période de suspension.

3. Les titulaires de la certification notifient aux acheteurs des produits TIC concernés la suspension et les raisons invoquées par l'organisme de certification pour justifier la suspension, à l'exception de celles dont la divulgation constituerait un risque pour la sécurité ou qui contiennent des informations sensibles. Ces informations sont également mises à la disposition du public par le titulaire du certificat.

4. Lorsqu'une autre législation pertinente de l'Union prévoit une présomption de conformité fondée sur des certificats délivrés en vertu des dispositions du présent règlement, l'autorité nationale de certification de cybersécurité informe l'autorité de surveillance du marché responsable de cette autre législation pertinente de l'Union de la suspension.

5. La suspension d'un certificat est notifiée à l'ENISA conformément à l'article 42, paragraphe 3.

6. Dans des cas dûment justifiés, l'autorité nationale de certification de cybersécurité peut autoriser une prolongation de la période de suspension d'un certificat EUCC. La période totale de suspension ne peut dépasser un an.

Article 31

Conséquences de la non-conformité de l'organisme d'évaluation de la conformité

1. Si un organisme de certification, ou l'organisme de certification concerné en cas de non-conformité d'un CESTI, ne respecte pas ses obligations, l'autorité nationale de certification de cybersécurité procède aux actions suivantes, dans les meilleurs délais:

a) identifier, avec l'aide du CESTI concerné, les certificats EUCC potentiellement concernés;

b) demander, le cas échéant, que des opérations d'évaluation soient effectuées sur un ou plusieurs produits TIC ou profils de protection, soit par le CESTI qui a procédé à l'évaluation, soit par tout autre CESTI accrédité et, le cas échéant, autorisé qui pourrait être le mieux placé techniquement pour aider à cette identification;

c) analyser les conséquences de cette non-conformité;

d) notifier le titulaire du certificat EUCC concerné par cette non-conformité.

2. Sur la base des mesures visées au paragraphe 1, l'organisme de certification adopte l'une ou l'autre des décisions suivantes pour chaque certificat EUCC concerné:

a) maintenir le certificat EUCC en l'état;

b) retirer le certificat EUCC conformément à l'article 14 ou 20 et, le cas échéant, délivrer un nouveau certificat EUCC.

3. Sur la base des mesures visées au paragraphe 1, l'autorité nationale de certification de cybersécurité:

a) signale, le cas échéant, à l'organisme national d'accréditation la non-conformité de l'organisme de certification ou du CESTI correspondant;

b) évalue, le cas échéant, l'incidence potentielle sur l'autorisation.

CHAPITRE VI

GESTION ET DIVULGATION DES VULNÉRABILITÉS

Article 32

Périmètre de la gestion des vulnérabilités

Le présent chapitre s'applique aux produits TIC pour lesquels un certificat EUCC a été délivré.

SECTION I

Gestion des vulnérabilités

Article 33

Procédures de gestion des vulnérabilités

1. Le titulaire d'un certificat EUCC établit et tient à jour toutes les procédures de gestion des vulnérabilités nécessaires conformément aux règles énoncées dans la présente section et, le cas échéant, complétées par les procédures définies dans la norme EN ISO/IEC 30111.

2. Le titulaire d'un certificat EUCC tient à jour et publie des méthodes appropriées pour recevoir des informations sur les vulnérabilités liées à ses produits de la part de sources externes, y compris les utilisateurs, les organismes de certification et les chercheurs dans le domaine de la sécurité.

3. Lorsque le titulaire d'un certificat EUCC détecte ou reçoit des informations sur une vulnérabilité potentielle touchant un produit TIC certifié, il l'enregistre et procède à une analyse d'impact de la vulnérabilité.

4. Lorsqu'une vulnérabilité potentielle a une incidence sur un produit composite, le titulaire du certificat EUCC informe de cette vulnérabilité potentielle le titulaire de certificats EUCC dépendants.

5. En réponse à une demande raisonnable de l'organisme de certification qui a délivré le certificat, le titulaire d'un certificat EUCC transmet toutes les informations pertinentes concernant les vulnérabilités potentielles à cet organisme de certification.

Article 34

Analyse d'impact des vulnérabilités

1. L'analyse d'impact d'une vulnérabilité fait référence à la cible d'évaluation et aux déclarations d'assurance figurant dans le certificat. L'analyse de l'impact d'une vulnérabilité est effectuée dans un délai adapté à l'exploitabilité et à la criticité de la vulnérabilité potentielle du produit TIC certifié.

2. Le cas échéant, un calcul du potentiel d'attaque est effectué selon la méthode pertinente incluse dans les normes visées à l'article 3 et aux documents de référence pertinents énumérés à l'annexe I, afin de déterminer l'exploitabilité de la vulnérabilité. Le niveau AVA_VAN du certificat EUCC est pris en compte.

Article 35

Rapport d'analyse d'impact des vulnérabilités

1. Le titulaire établit un rapport d'analyse d'impact d'une vulnérabilité lorsque l'analyse d'impact montre qu'une vulnérabilité a une incidence probable sur la conformité du produit TIC avec son certificat.

2. Le rapport d'analyse d'impact d'une vulnérabilité contient l'évaluation des éléments suivants:

a) l'incidence de la vulnérabilité sur le produit TIC certifié;

b) les risques éventuels liés à la proximité ou à la disponibilité d'une attaque;

c) la possibilité de remédier à la vulnérabilité;

d) s'il est possible de remédier à la vulnérabilité, les résolutions possibles de cette vulnérabilité.

3. Le rapport d'analyse d'impact d'une vulnérabilité contient, le cas échéant, des détails sur les moyens d'exploitation possibles de la vulnérabilité. Les informations relatives aux moyens d'exploitation possibles de la vulnérabilité sont traitées conformément aux mesures de sécurité appropriées afin de protéger leur confidentialité et de garantir, le cas échéant, leur diffusion limitée.

4. Le titulaire d'un certificat EUCC transmet sans retard injustifié le rapport d'analyse d'impact d'une vulnérabilité à l'organisme de certification ou à l'autorité nationale de certification de cybersécurité conformément à l'article 56, paragraphe 8, du règlement (UE) 2019/881.

5. Lorsque le rapport d'analyse d'impact d'une vulnérabilité établit que la vulnérabilité n'est pas résiduelle au sens des normes visées à l'article 3 et qu'il est possible d'y remédier, l'article 36 s'applique.

6. Lorsque le rapport d'analyse d'impact d'une vulnérabilité établit que la vulnérabilité n'est pas résiduelle et qu'il n'est pas possible d'y remédier, le certificat EUCC est retiré conformément à l'article 14.

7. Le titulaire du certificat EUCC surveille les éventuelles vulnérabilités résiduelles afin de s'assurer qu'elles ne pourront pas être exploitées en cas de modification de l'environnement opérationnel.

Article 36

Résolution des vulnérabilités

Le titulaire du certificat EUCC soumet une proposition de mesure corrective appropriée à l'organisme de certification. L'organisme de certification réexamine le certificat conformément à l'article 13. La portée de ce réexamen est déterminée par la mesure proposée pour remédier à la vulnérabilité.

SECTION II

Divulgation des vulnérabilités

Article 37

Informations communiquées à l'autorité nationale de certification de cybersécurité

1. Les informations fournies par l'organisme de certification à l'autorité nationale de certification de cybersécurité comprennent tous les éléments nécessaires à l'autorité nationale de certification de cybersécurité pour comprendre l'incidence de la vulnérabilité, les changements à apporter au produit TIC et, le cas échéant, toute information provenant de l'organisme de certification sur les implications au sens large de la vulnérabilité pour d'autres produits TIC certifiés.

2. Les informations fournies conformément au paragraphe 1 ne contiennent pas de précisions sur les moyens d'exploitation de la vulnérabilité. La présente disposition est sans préjudice des pouvoirs d'enquête de l'autorité nationale de certification de cybersécurité.

Article 38

Coopération avec d'autres autorités nationales de certification de cybersécurité

1. L'autorité nationale de certification de cybersécurité communique les informations pertinentes reçues conformément à l'article 37 aux autres autorités nationales de certification de cybersécurité et à l'ENISA.

2. D'autres autorités nationales de certification de cybersécurité peuvent décider de poursuivre l'analyse de la vulnérabilité ou, après avoir informé le titulaire du certificat EUCC, demander aux organismes de certification concernés d'évaluer si la vulnérabilité peut avoir une incidence sur d'autres produits TIC certifiés.

Article 39

Publication de la vulnérabilité

Dès le retrait d'un certificat, le titulaire du certificat EUCC divulgue et enregistre toute vulnérabilité du produit TIC connue du public et corrigée, soit dans la base de données européenne des vulnérabilités établie conformément à l'article 12 de la

directive (UE) 2022/2555 du Parlement européen et du Conseil ([5]), soit dans les autres répertoires en ligne visés à l'article 55, paragraphe 1, point d), du règlement (UE) 2019/881.

CHAPITRE VII

CONSERVATION, DIVULGATION ET PROTECTION DES INFORMATIONS

Article 40

Conservation des archives par les organismes de certification et les CESTI

1. Les CESTI et les organismes de certification ont un système d'archivage contenant tous les documents créés dans le cadre de chaque évaluation et certification qu'ils effectuent.

2. Les organismes de certification et les CESTI stockent les archives en toute sécurité et les conservent pendant la période nécessaire aux fins du présent règlement et pendant au moins cinq ans après le retrait des certificats EUCC concernés. Lorsque l'organisme de certification a délivré un nouveau certificat EUCC conformément à l'article 13, paragraphe 2, point c), il conserve, avec ce nouveau certificat EUCC et pour la même durée, la documentation du certificat EUCC retiré.

Article 41

Informations mises à disposition par le titulaire d'un certificat

1. Les informations visées à l'article 55 du règlement (UE) 2019/881 sont rendues disponibles dans un langage aisément accessible aux utilisateurs.

2. Le titulaire d'un certificat EUCC conserve les éléments suivants de manière sécurisée pendant la période nécessaire aux fins du présent règlement et pendant au moins cinq ans après le retrait du certificat EUCC concerné:

a) les archives des informations fournies à l'organisme de certification et au CESTI au cours de la procédure de certification;

b) un spécimen du produit TIC certifié.

3. Lorsque l'organisme de certification a délivré un nouveau certificat EUCC conformément à l'article 13, paragraphe 2, point c), le titulaire conserve, avec ce nouveau certificat EUCC et pour la même durée, la documentation du certificat EUCC retiré.

4. À la demande de l'organisme de certification ou de l'autorité nationale de certification de cybersécurité, le titulaire d'un certificat EUCC met à disposition les archives et les copies visées au paragraphe 2.

Article 42

Informations mises à disposition par l'ENISA

1. L'ENISA publie les informations suivantes sur le site web visé à l'article 50, paragraphe 1, du règlement (UE) 2019/881:

a) tous les certificats EUCC;

b) les informations relatives au statut d'un certificat EUCC, notamment celles permettant de savoir s'il est valide ou s'il a été suspendu, retiré ou expiré;

c) les rapports de certification correspondant à chaque certificat EUCC;

([5]) Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

d) la liste des organismes d'évaluation de la conformité accrédités;

e) la liste des organismes d'évaluation de la conformité autorisés;

f) les documents de référence énumérés à l'annexe I;

g) les avis du groupe européen de certification de cybersécurité visés à l'article 62, paragraphe 4, point c), du règlement (UE) 2019/881;

h) les rapports d'évaluation par les pairs établis conformément à l'article 47.

2. Les informations visées au paragraphe 1 sont mises à disposition au moins en anglais.

3. Les organismes de certification et, le cas échéant, les autorités nationales de certification de cybersécurité informent l'ENISA dans les meilleurs délais de leurs décisions affectant le contenu ou le statut d'un certificat EUCC visé au paragraphe 1, point b).

4. L'ENISA veille à ce que les informations publiées en vertu du paragraphe 1, points a), b) et c), identifient clairement les versions d'un produit TIC certifié qui sont couvertes par un certificat EUCC.

Article 43

Protection de l'information

Les organismes d'évaluation de la conformité, les autorités nationales de certification de cybersécurité, le GECC, l'ENISA, la Commission et toutes les autres parties veillent à la sécurité et à la protection des secrets d'affaires et autres informations confidentielles, y compris les secrets commerciaux, ainsi qu'à la préservation des droits de propriété intellectuelle, et prennent les mesures techniques et organisationnelles nécessaires et appropriées.

CHAPITRE VIII

ACCORDS DE RECONNAISSANCE MUTUELLE AVEC DES PAYS TIERS

Article 44

Conditions

1. Les pays tiers qui souhaitent certifier leurs produits conformément au présent règlement et qui souhaitent que cette certification soit reconnue dans l'Union concluent un accord de reconnaissance mutuelle avec l'Union.

2. L'accord de reconnaissance mutuelle couvre les niveaux d'assurance applicables aux produits TIC certifiés et, le cas échéant, aux profils de protection.

3. Les accords de reconnaissance mutuelle visés au paragraphe 1 ne peuvent être conclus qu'avec des pays tiers qui:

a) disposent d'une autorité qui:

   1) est un organisme public, indépendant, du point de vue de la structure organisationnelle et juridique, du financement et des prises de décisions, des entités qu'il supervise et contrôle;

   2) dispose de pouvoirs de contrôle et de surveillance appropriés pour mener des enquêtes et est habilitée à prendre des mesures correctives appropriées pour garantir la conformité;

   3) dispose d'un système de sanctions efficace, proportionné et dissuasif pour garantir la conformité;

   4) accepte de collaborer avec le groupe européen de certification de cybersécurité et l'ENISA pour échanger les meilleures pratiques et les évolutions pertinentes dans le domaine de la certification de cybersécurité et pour œuvrer à une interprétation uniforme des critères et méthodes d'évaluation actuellement applicables, notamment en appliquant une documentation harmonisée équivalente aux documents de référence énumérés à l'annexe I;

b) disposent d'un organisme d'accréditation indépendant effectuant des accréditations sur la base de normes équivalentes à celles visées dans le règlement (CE) nº 765/2008;

c) s'engagent à ce que les processus et procédures d'évaluation et de certification soient menés de manière dûment professionnelle, en tenant compte du respect des normes internationales visées dans le présent règlement, en particulier à l'article 3;

d) ont la capacité de signaler des vulnérabilités non détectées précédemment et ont établi une procédure adéquate de gestion et de divulgation des vulnérabilités;

e) ont mis en place des procédures leur permettant d'introduire et de traiter efficacement les plaintes et d'offrir un recours juridique effectif aux plaignants;

f) établissent un mécanisme de coopération avec d'autres organismes de l'Union et des États membres concernés par la certification de cybersécurité au titre du présent règlement, y compris le partage d'informations sur la non-conformité éventuelle des certificats, le suivi des évolutions pertinentes dans le domaine de la certification et l'adoption d'une approche commune en matière de maintien et d'examen de la certification.

4. Outre les conditions énoncées au paragraphe 3, un accord de reconnaissance mutuelle visé au paragraphe 1 et portant sur le niveau d'assurance «élevé» ne peut être conclu avec des pays tiers que si les conditions suivantes sont également remplies:

a) le pays tiers dispose d'une autorité de certification indépendante et publique en matière de cybersécurité qui effectue ou délègue les activités d'évaluation nécessaires pour autoriser la certification au niveau d'assurance «élevé», qui sont équivalentes aux exigences et aux procédures établies pour les autorités nationales de cybersécurité dans le présent règlement et dans le règlement (UE) 2019/881;

b) l'accord de reconnaissance mutuelle établit un mécanisme commun équivalent à l'évaluation par les pairs pour la certification EUCC afin de renforcer l'échange de pratiques et de résoudre conjointement les problèmes dans le domaine de l'évaluation et de la certification.

CHAPITRE IX

ÉVALUATION PAR LES PAIRS DES ORGANISMES DE CERTIFICATION

Article 45

Procédure d'évaluation par les pairs

1. Un organisme de certification délivrant des certificats EUCC de niveau d'assurance «élevé» fait l'objet d'une évaluation par les pairs à intervalles réguliers et au moins tous les cinq ans. Les différents types d'évaluation par les pairs figurent à l'annexe VI.

2. Le groupe européen de certification de cybersécurité établit et tient à jour un calendrier des évaluations par les pairs en veillant à ce que cette périodicité soit respectée. Sauf dans des cas dûment justifiés, les évaluations par les pairs sont effectuées sur place.

3. L'évaluation par les pairs peut s'appuyer sur des éléments de preuve recueillis au cours d'évaluations par les pairs antérieures ou de procédures équivalentes de l'organisme de certification évalué par les pairs ou de l'autorité nationale de certification de cybersécurité, à condition que:

a) les résultats ne datent pas de plus de cinq ans;

b) les résultats soient accompagnés d'une description des procédures d'évaluation par les pairs établies pour ce schéma lorsqu'ils se rapportent à une évaluation par les pairs réalisée dans le cadre d'un schéma de certification différent;

c) le rapport d'évaluation par les pairs visé à l'article 47 précise quels résultats ont été réutilisés avec ou sans nouvelle évaluation.

4. Lorsqu'une évaluation par les pairs couvre un domaine technique, le CESTI concerné est lui aussi évalué.

5. L'organisme de certification évalué par les pairs et, le cas échéant, l'autorité nationale de certification de cybersécurité veillent à ce que toutes les informations pertinentes soient mises à la disposition de l'équipe d'évaluation par les pairs.

6. L'évaluation par les pairs est effectuée par une équipe dédiée constituée comme indiqué à l'annexe VI.

Article 46

Phases d'évaluation par les pairs

1. Au cours de la phase préparatoire, les membres de l'équipe d'évaluation par les pairs examinent la documentation de l'organisme de certification portant sur ses politiques et procédures, y compris l'utilisation de documents de référence.

2. Au cours de la phase de visite du site, l'équipe d'évaluation par les pairs évalue la compétence technique de l'organisme et, le cas échéant, la compétence d'un CESTI qui a réalisé au moins une évaluation de produit TIC couverte par l'évaluation par les pairs.

3. La durée de la phase de visite du site peut être prolongée ou réduite en fonction de facteurs tels que la possibilité de réutiliser des preuves et des résultats d'une évaluation par les pairs existante ou le nombre de CESTI et de domaines techniques pour lesquels l'organisme de certification délivre des certificats.

4. Le cas échéant, l'équipe d'évaluation par les pairs détermine la compétence technique de chaque CESTI en visitant son ou ses laboratoires techniques et en s'entretenant avec les évaluateurs en ce qui concerne le domaine technique et les méthodes d'attaque spécifiques qui s'y rapportent.

5. Au cours de la phase d'établissement du rapport, l'équipe d'évaluation consigne ses constatations dans un rapport d'évaluation par les pairs comprenant un verdict et, le cas échéant, la liste des non-conformités observées, chacune classée selon un niveau de criticité.

6. Le rapport d'évaluation par les pairs doit d'abord faire l'objet de discussions avec l'organisme de certification évalué par les pairs. À la suite de ces discussions, l'organisme de certification évalué par les pairs établit un calendrier des mesures à prendre pour donner suite aux constatations.

Article 47

Rapport d'évaluation par les pairs

1. L'équipe d'évaluation par les pairs fournit à l'organisme de certification évalué par les pairs un projet de rapport d'évaluation par les pairs.

2. L'organisme de certification évalué par les pairs soumet à l'équipe d'évaluation par les pairs des observations concernant les constatations et une liste d'engagements visant à remédier aux lacunes recensées dans le projet de rapport d'évaluation par les pairs.

3. L'équipe d'évaluation par les pairs soumet au groupe européen de certification de cybersécurité un rapport final d'évaluation par les pairs, qui comprend également les commentaires formulés et les engagements pris par l'organisme de certification évalué par les pairs. L'équipe d'évaluation par les pairs fait également part de sa position quant aux commentaires et indique si les engagements sont suffisants pour remédier aux lacunes constatées.

4. Lorsque des non-conformités sont recensées dans le rapport d'évaluation par les pairs, le groupe européen de certification de cybersécurité peut fixer un délai approprié pour que l'organisme de certification évalué par les pairs remédie à ces non-conformités.

5. Le groupe européen de certification de cybersécurité adopte un avis sur le rapport d'évaluation par les pairs:

a) lorsque le rapport d'évaluation par les pairs ne recense pas de non-conformités ou lorsque les non-conformités ont été traitées de manière appropriée par l'organisme de certification évalué par les pairs, le groupe européen de certification de cybersécurité peut émettre un avis positif et tous les documents pertinents sont publiés sur le site web de certification de l'ENISA;

b) lorsque l'organisme de certification évalué par les pairs ne traite pas les non-conformités de manière appropriée dans le délai imparti, le groupe européen de certification de cybersécurité peut émettre un avis négatif à publier sur le site web de certification de l'ENISA, avec le rapport d'évaluation par les pairs et tous les documents pertinents.

6. Avant la publication de l'avis, toutes les informations sensibles, personnelles ou propriétaires sont retirées des documents publiés.

CHAPITRE X

MAINTIEN DU SCHÉMA

Article 48

Maintenance de l'EUCC

1. La Commission peut demander au groupe européen de certification de cybersécurité d'adopter un avis en vue de tenir à jour le schéma EUCC et d'entreprendre les travaux préparatoires nécessaires.

2. Le groupe européen de certification de cybersécurité peut adopter un avis afin d'approuver des documents de référence.

3. Les documents de référence qui ont été approuvés par le groupe européen de certification de cybersécurité sont publiés par l'ENISA.

CHAPITRE XI

DISPOSITIONS FINALES

Article 49

Schémas nationaux couverts par l'EUCC

1. Conformément à l'article 57, paragraphe 1, du règlement (UE) 2019/881 et sans préjudice de l'article 57, paragraphe 3, dudit règlement, tous les schémas nationaux de certification de cybersécurité et les procédures connexes pour les produits TIC et les processus TIC qui sont couverts par le schéma EUCC cessent de produire leurs effets 12 mois après l'entrée en vigueur du présent règlement.

2. Par dérogation à l'article 50, un processus de certification peut être engagé dans le cadre d'un schéma national de certification de cybersécurité dans les 12 mois suivant l'entrée en vigueur du présent règlement, pour autant qu'il soit achevé au plus tard 24 mois après celle-ci.

3. Les certificats délivrés en vertu de schémas nationaux de certification de cybersécurité peuvent faire l'objet d'un réexamen. Les nouveaux certificats remplaçant les certificats réexaminés sont délivrés conformément au présent règlement.

Article 50

Entrée en vigueur

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

Il est applicable à partir du 27 février 2025.

Le chapitre IV et l'annexe V sont applicables à partir de la date d'entrée en vigueur du présent règlement.

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

Fait à Bruxelles, le 31 janvier 2024.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE I

Domaines techniques et documents de référence

1. Domaines techniques au niveau AVA_VAN 4 ou 5:

   a) les documents relatifs à l'évaluation harmonisée du domaine technique «cartes à puce et dispositifs similaires» et en particulier les documents suivants, dans leurs versions respectives en vigueur le [date d'entrée en vigueur]:

      1) «Minimum ITSEF requirements for security evaluations of smart cards and similar devices», initialement approuvé par le GECC le 20 octobre 2023;

      2) «Minimum Site Security Requirements», initialement approuvé par le GECC le 20 octobre 2023;

      3) «Application of Common Criteria to integrated circuits», initialement approuvé par le GECC le 20 octobre 2023;

      4) «Security Architecture requirements (ADV_ARC) for smart cards and similar devices», initialement approuvé par le GECC le 20 octobre 2023;

      5) «Certification of "open" smart card products», initialement approuvé par le GECC le 20 octobre 2023;

      6) «Composite product evaluation for smart cards and similar devices», initialement approuvé par le GECC le 20 octobre 2023;

      7) «Application of Attack Potential to Smartcards», initialement approuvé par le GECC le 20 octobre 2023;

   b) les documents relatifs à l'évaluation harmonisée du domaine technique «dispositifs matériels avec boîtiers de sécurité» et en particulier les documents suivants, dans leurs versions respectives en vigueur le [date d'entrée en vigueur]:

      1) «Minimum ITSEF requirements for security evaluations of hardware devices with security boxes», initialement approuvé par le GECC le 20 octobre 2023;

      2) «Minimum Site Security Requirements», initialement approuvé par le GECC le 20 octobre 2023;

      3) «Application of Attack Potential to hardware devices with security boxes», initialement approuvé par le GECC le 20 octobre 2023.

2. Les documents de référence dans leurs versions respectives en vigueur le [date d'entrée en vigueur]:

   a) document relatif à l'accréditation harmonisée des organismes d'évaluation de la conformité: «Accreditation of ITSEFs for the EUCC», initialement approuvé par le GECC le 20 octobre 2023.

ANNEXE II

Profils de protection certifiés au niveau AVA_VAN 4 ou 5

1. Pour la catégorie des dispositifs de création de signature ou de cachet électronique qualifiés à distance:

1) EN 419241-2:2019 — Systèmes fiables prenant en charge la signature de serveur — Partie 2: Profils de protection de QSCD pour la signature par serveur;

2) EN 419221-5:2018 — Profils de protection pour les modules cryptographiques de prestataires de services de confiance — Partie 5: Module cryptographique pour services de confiance.

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

[VIERGE]

ANNEXE III

Profils de protection recommandés (illustrant les domaines techniques répertoriés à l'annexe I)

Profils de protection utilisés dans la certification des produits TIC entrant dans les catégories de produits TIC ci-dessous:

a) pour la catégorie des documents de voyage lisibles à la machine:

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

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

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

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

b) pour la catégorie des dispositifs sécurisés de création de signature:

1) EN 419211-1:2014 — Profils de protection pour dispositif sécurisé de création de signature électronique — Partie 1: Présentation générale;

2) EN 419211-2:2013 — Profils de protection des dispositifs sécurisés de création de signature — Partie 2: Dispositif avec génération de clé;

3) EN 419211-3:2013 — Profils de protection des dispositifs sécurisés de création de signature — Partie 3: Dispositif avec import de clé;

4) EN 419211-4:2013 — Profils de protection des dispositifs sécurisés de création de signature — Partie 4: Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de génération de certificats;

5) EN 419211-5:2013 — Profils de protection des dispositifs sécurisés de création de signature — Partie 5: Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de création de signature;

6) EN 419211-6:2014 — Profils de protection des dispositifs sécurisés de création de signature — Partie 6: Extension pour un dispositif avec import de clé et communication sécurisée avec l'application de création de signature;

c) pour la catégorie des tachygraphes numériques:

1) Tachygraphe numérique — Carte tachygraphique, telle que visée dans le règlement d'exécution (UE) 2016/799 de la Commission du 18 mars 2016 mettant en œuvre le règlement (UE) n° 165/2014 (annexe 1C);

2) Tachygraphe numérique — Unité embarquée sur le véhicule telle que visée à l'annexe IB du règlement (CE) n° 1360/2002 de la Commission, conçue pour être installée sur des véhicules de transport routier;

3) Tachygraphe numérique — Dispositif GNSS externe (EGF PP) tel que visé à l'annexe 1C du 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;

4) Tachygraphe numérique — Capteur de mouvement (MS PP) tel que visé à l'annexe 1C du 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;

d) pour la catégorie des circuits intégrés sécurisés, des cartes à puce et des dispositifs connexes:

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

2) Java Card System - Open Configuration, V3.0.5 BSI-CC-PP-0099-2017;

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

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

5) Universal SIM card, PU-2009-RT-79, ANSSI-CC-PP-2010/04;

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

e) pour la catégorie des points d'interaction (de paiement) et des terminaux de paiement:

1) Point d'interaction «POI-CHIP-ONLY», ANSSI-CC-PP-2015/01;

2) Point d'interaction «POI-CHIP-ONLY and Open Protocol Package», ANSSI-CC-PP-2015/02;

3) Point d'interaction «POI-COMPREHENSIVE», ANSSI-CC-PP-2015/03;

4) Point d'interaction «POI-COMPREHENSIVE and Open Protocol Package», ANSSI-CC-PP-2015/04;

5) Point d'interaction «POI-PED-ONLY», ANSSI-CC-PP-2015/05;

6) Point d'interaction «POI-PED-ONLY and Open Protocol Package», ANSSI-CC-PP-2015/06;

f) pour la catégorie des dispositifs matériels avec boîtiers de sécurité:

1) Cryptographic Module for CSP Signing Operations with Backup — PP CMCSOB, PP HSM CMCSOB 14167-2, ANSSI-CC-PP-2015/08;

2) Cryptographic Module for CSP key generation services — PP CMCKG, PP HSM CMCKG 14167-3, ANSSI-CC-PP-2015/09;

3) Cryptographic Module for CSP Signing Operations without Backup — PP CMCSO, PP HSM CMCKG 14167-4, ANSSI-CC-PP-2015/10.

ANNEXE IV

Continuité de l'assurance et réexamen des certificats

IV.1 **Continuité de l'assurance: portée**

1. Les exigences suivantes en matière de continuité de l'assurance s'appliquent aux activités de maintenance liées à ce qui suit:

   a) une réévaluation pour savoir si un produit TIC certifié inchangé répond encore aux exigences de sécurité correspondantes;

   b) une évaluation de l'incidence des changements apportés à un produit TIC certifié sur sa certification;

   c) si elle est incluse dans la certification, l'application de correctifs conformément à un processus de gestion des correctifs évalué;

   d) s'il est inclus, le réexamen des processus de production ou de gestion du cycle de vie du titulaire du certificat.

2. Le titulaire d'un certificat EUCC peut demander le réexamen du certificat dans les cas suivants:

   a) le certificat EUCC expire dans les neuf mois;

   b) un changement apporté au produit TIC certifié ou à un autre facteur pourrait avoir une incidence sur la fonctionnalité de sécurité du produit;

   c) le titulaire du certificat exige que l'évaluation de la vulnérabilité soit effectuée à nouveau afin de reconfirmer l'assurance du certificat EUCC associée à la résistance du produit TIC contre les cyberattaques actuelles.

IV.2 **Réévaluation**

1. Lorsqu'il est nécessaire d'évaluer l'incidence des changements dans l'environnement des menaces d'un produit TIC certifié inchangé, une demande de réévaluation est soumise à l'organisme de certification.

2. La réévaluation est effectuée par le CESTI qui a réalisé l'évaluation précédente, en réutilisant tous les résultats qui s'appliquent encore. L'évaluation se concentre sur les activités d'assurance qui sont potentiellement affectées par la modification de l'environnement de menaces lié au produit TIC certifié, en particulier la famille AVA_VAN concernée et, en outre, la famille du cycle de vie de l'assurance (ALC) où des preuves suffisantes relatives à la maintenance de l'environnement de développement sont à nouveau collectées.

3. Le CESTI décrit les changements et détaille les résultats de la réévaluation avec une mise à jour du rapport technique d'évaluation précédent.

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.

5. Le rapport de réévaluation et le certificat mis à jour sont fournis à l'autorité nationale de certification de cybersécurité, ainsi qu'à l'ENISA pour publication sur son site web consacré à la certification de cybersécurité.

IV.3 **Modification d'un produit TIC certifié**

1. Lorsqu'un produit TIC certifié a fait l'objet de modifications, le titulaire du certificat qui souhaite tenir à jour ce certificat fournit à l'organisme de certification un rapport d'analyse d'impact.

2. Le rapport d'analyse d'impact contient les éléments suivants:

   a) une introduction contenant les informations nécessaires pour identifier le rapport d'analyse d'impact et la cible d'évaluation soumise à des modifications;

b) une description des modifications apportées au produit;

c) le recensement des éléments de preuve du développeur concernés;

d) une description des modifications apportées aux éléments de preuve du développeur;

e) les constatations et les conclusions relatives à l'incidence sur l'assurance pour chaque modification.

3. L'organisme de certification examine les modifications décrites dans le rapport d'analyse d'impact afin de valider leur incidence sur l'assurance de la cible d'évaluation certifiée, comme proposé dans les conclusions du rapport d'analyse d'impact.

4. À l'issue de cet examen, l'organisme de certification détermine si l'ampleur d'une modification est mineure ou majeure en fonction de son incidence.

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

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

1) introduction;

2) description des modifications;

3) éléments de preuve du développeur concerné;

b) la date de validité du nouveau certificat ne dépasse pas la date du certificat initial.

6. Le nouveau certificat, y compris le rapport de maintenance, est fourni à l'ENISA pour publication sur son site web de certification de cybersécurité.

7. Lorsque les modifications sont considérées comme majeures, une réévaluation est effectuée dans le contexte de l'évaluation précédente et en réutilisant tous les résultats de l'évaluation précédente qui s'appliquent encore.

8. Une fois l'évaluation de la nouvelle cible d'évaluation terminée, le CESTI établit un nouveau rapport technique d'évaluation. L'organisme de certification examine le rapport technique d'évaluation mis à jour et, le cas échéant, établit un nouveau certificat accompagné d'un nouveau rapport de certification.

9. Le nouveau certificat et le nouveau rapport de certification sont transmis à l'ENISA pour publication.

IV.4 **Gestion des correctifs**

1. Une procédure de gestion des correctifs prévoit un processus structuré de mise à jour d'un produit TIC certifié. La procédure de gestion des correctifs, y compris le mécanisme tel qu'il est mis en œuvre dans le produit TIC par le candidat à la certification, peut être utilisée après la certification du produit TIC sous la responsabilité de l'organisme d'évaluation de la conformité.

2. Le candidat à la certification peut inclure dans la certification du produit TIC un mécanisme de correctif dans le cadre d'une procédure de gestion certifiée mise en œuvre dans le produit TIC dans l'une des conditions suivantes:

a) les fonctionnalités concernées par le correctif sont en dehors de la cible d'évaluation du produit TIC certifié;

b) le correctif concerne une modification mineure prédéterminée du produit TIC certifié;

c) le correctif concerne une vulnérabilité confirmée ayant des effets critiques sur la sécurité du produit TIC certifié.

3. Si le correctif concerne une modification majeure de la cible d'évaluation du produit TIC certifié, en lien avec une vulnérabilité non détectée précédemment et n'ayant pas d'effets critiques sur la sécurité du produit TIC, les dispositions de l'article 13 s'appliquent.

4. La procédure de gestion des correctifs pour un produit TIC se compose des éléments suivants:

   a) le processus de développement et de publication du correctif pour le produit TIC;

   b) le mécanisme technique et les fonctions pour l'adoption du correctif dans le produit TIC;

   c) un ensemble d'activités d'évaluation liées à l'efficacité et à la performance du mécanisme technique.

5. Au cours de la certification du produit TIC:

   a) le candidat à la certification du produit TIC fournit la description de la procédure de gestion des correctifs;

   b) le CESTI vérifie les éléments suivants:

      1) le développeur a mis en œuvre les mécanismes de correctifs dans le produit TIC conformément à la procédure de gestion des correctifs qui a été soumise à la certification;

      2) les limites de la cible d'évaluation sont séparées de manière que les modifications apportées aux processus séparés n'affectent pas la sécurité de la cible d'évaluation;

      3) le mécanisme de correctif technique fonctionne conformément aux dispositions de la présente section et aux déclarations du demandeur;

   c) l'organisme de certification inclut dans le rapport de certification le résultat de l'évaluation de la procédure de gestion des correctifs.

6. Le titulaire du certificat peut appliquer au produit TIC certifié concerné le correctif créé conformément à la procédure certifiée de gestion des correctifs et prend les mesures suivantes dans un délai de 5 jours ouvrables dans les cas suivants:

   a) dans le cas visé au point 2 a), il signale le correctif concerné à l'organisme de certification qui ne modifie pas le certificat EUCC correspondant;

   b) dans le cas visé au point 2 b), il soumet le correctif concerné au CESTI pour examen. Le CESTI informe l'organisme de certification de la réception du correctif, après quoi l'organisme de certification prend les mesures appropriées pour délivrer une nouvelle version du certificat EUCC correspondant et pour mettre à jour le rapport de certification;

   c) dans le cas visé au point 2 c), il soumet le correctif concerné au CESTI pour la réévaluation nécessaire, mais peut déployer le correctif en parallèle. Le CESTI en informe l'organisme de certification, après quoi ce dernier entame les activités de certification correspondantes.

ANNEXE V

Contenu d'un rapport de certification

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 correspondant.

2. Le rapport de certification est une source d'informations détaillées et pratiques sur le produit TIC ou la catégorie de produits 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 sections suivantes:

   a) un résumé;

   b) l'identification du produit TIC ou de la catégorie de produits TIC pour les profils de protection;

   c) les services de sécurité;

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

   e) les informations architecturales;

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

   g) les essais du produit TIC, s'ils ont été effectués;

   h) le cas échéant, une identification des installations de production et des processus de gestion du cycle de vie du titulaire du certificat;

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

   j) un résumé de la cible de sécurité du produit TIC soumis à la certification;

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

   l) une bibliographie.

4. Le résumé est une brève synthèse de l'ensemble du rapport de certification. Le résumé fournit un aperçu clair et concis des résultats de l'évaluation et inclut les informations suivantes:

   a) le nom du produit TIC évalué, l'énumération des composants du produit qui font partie de l'évaluation et la version du produit TIC;

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

   c) la date de fin de l'évaluation;

   d) la référence au rapport technique d'évaluation établi par le CESTI;

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

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

      2) les composants d'assurance de sécurité et le paquet d'assurance 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;

      3) la fonctionnalité de sécurité du produit TIC évalué;

      4) un résumé des menaces et des politiques de sécurité organisationnelles traitées par le produit TIC évalué;

5) les exigences particulières de configuration;

6) les hypothèses relatives à l'environnement d'exploitation;

7) le cas échéant, la procédure de gestion des correctifs approuvée conformément à la section IV.4 de l'annexe IV;

8) la ou les clauses de non-responsabilité.

5. Le produit TIC évalué est clairement identifié, y compris en indiquant les informations suivantes:

a) le nom du produit TIC évalué;

b) l'énumération des composants du produit TIC qui font partie de l'évaluation;

c) le numéro de version des composants du produit TIC;

d) l'identification des exigences supplémentaires relatives à l'environnement d'exploitation du produit TIC certifié;

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

f) le cas échéant, la procédure de gestion des correctifs incluse dans le certificat;

g) le lien vers le site web du titulaire du certificat EUCC où sont fournies des informations supplémentaires en matière de cybersécurité pour le produit TIC certifié conformément à l'article 55 du règlement (UE) 2019/881.

6. Les informations incluses dans la présente section sont aussi précises que possible afin de garantir une représentation complète et exacte du produit TIC qui puisse être réutilisée dans des évaluations futures.

7. La section relative à la politique de sécurité contient la description de la politique de sécurité du produit TIC et les politiques ou règles que le produit TIC évalué met en œuvre ou auxquelles il se conforme. Elle inclut une référence et une description des politiques suivantes:

a) la politique de traitement des vulnérabilités du titulaire du certificat;

b) la politique de continuité de l'assurance du titulaire du certificat.

8. Le cas échéant, la politique peut inclure les conditions relatives à l'utilisation d'une procédure de gestion des correctifs pendant la durée de validité du certificat.

9. La section relative aux hypothèses et aux éclaircissements quant au champ d'application contient des informations exhaustives concernant les circonstances et les objectifs liés à l'utilisation prévue du produit telle que visée à l'article 7, paragraphe 1, point c). Ces informations comprennent:

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.

10. Les informations énumérées au point 9 sont aussi claires que possible afin que les utilisateurs du produit TIC certifié puissent prendre des décisions éclairées par rapport aux risques associés à son utilisation.

11. La section relative aux informations architecturales comprend une description détaillée du produit TIC et de ses principaux composants conformément à la conception des sous-systèmes ADV_TDS des critères communs.

12. La liste complète des informations supplémentaires sur la cybersécurité du produit TIC est fournie conformément à l'article 55 du règlement (UE) 2019/881. Toute la documentation pertinente est identifiée par les numéros de version.

13. La section relative aux essais du produit TIC comprend les informations suivantes:

    a) le nom et le point de contact de l'autorité ou de l'organisme qui a délivré le certificat, y compris l'autorité nationale de certification de cybersécurité compétente;

    b) le nom du CESTI qui a réalisé l'évaluation, lorsqu'il s'agit d'un organisme différent de l'organisme de certification;

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

    d) la version du document de référence et les autres critères d'évaluation de la sécurité utilisés dans l'évaluation;

    e) les paramètres et la configuration complets et précis du produit TIC pendant l'évaluation, y compris les notes et observations opérationnelles si elles sont disponibles;

    f) tout profil de protection utilisé, y compris les informations suivantes:

        1) l'auteur du profil de protection;

        2) le nom et l'identifiant du profil de protection;

        3) l'identifiant du certificat du profil de protection;

        4) le nom et les coordonnées de l'organisme de certification et du CESTI ayant participé à l'évaluation du profil de protection;

        5) le(s) paquet(s) d'assurance requis pour un produit conforme au profil de protection.

14. Les résultats de l'évaluation et les informations relatives à la section du certificat comprennent les informations suivantes:

    a) la confirmation du niveau d'assurance atteint, tel que visé à l'article 4 du présent règlement et à l'article 52 du règlement (UE) 2019/881;

    b) les exigences d'assurance des normes visées à l'article 3 auxquelles le produit TIC ou le profil de protection répond effectivement, y compris le niveau AVA_VAN;

    c) une description détaillée des exigences d'assurance, ainsi que des détails sur la manière dont le produit satisfait à chacune d'entre elles;

    d) la date de délivrance et la durée de validité du certificat;

    e) l'identifiant unique du certificat.

15. La cible de sécurité est incluse dans le rapport de certification ou référencée et résumée dans le rapport de certification et fournie avec le rapport de certification aux fins de publication.

16. La cible de sécurité peut être assainie conformément à la section VI.2.

17. La marque ou l'étiquette associée au schéma EUCC peut être insérée dans le rapport de certification conformément aux règles et procédures prévues à l'article 11.

18. La section de la bibliographie 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, ainsi que leur version;

    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) la documentation du développeur utilisée dans le cadre de l'évaluation.

19. 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.

V.2 **Assainissement d'une cible de sécurité en vue de sa publication**

1. La cible de sécurité à inclure dans le rapport de certification ou à laquelle ce dernier fait référence conformément à la section VI.1, point 1, peut être assainie en supprimant ou en paraphrasant des informations techniques exclusives.

2. La cible de sécurité assainie qui en résulte est une représentation réelle de sa version originale complète. Cela signifie que la cible de sécurité assainie ne peut pas omettre d'informations nécessaires à la compréhension des propriétés de sécurité de la cible d'évaluation et de la portée de l'évaluation.

3. Le contenu de la cible de sécurité assainie est conforme aux exigences minimales suivantes:
   a) l'introduction n'est pas assainie car elle ne contient pas d'informations exclusives en général;
   b) la cible de sécurité assainie doit avoir un identifiant unique distinct de sa version originale complète;
   c) la description de la cible d'évaluation peut être réduite car elle peut inclure des informations exclusives et détaillées sur la conception de la cible d'évaluation qui ne devraient pas être publiées;
   d) la description de l'environnement de sécurité de la cible d'évaluation (hypothèses, menaces, politiques de sécurité de l'organisation) n'est pas réduite dans la mesure où cette information est nécessaire pour comprendre la portée de l'évaluation;
   e) les objectifs de sécurité ne sont pas réduits, car toutes les informations doivent être rendues publiques pour comprendre l'intention de la cible de sécurité et de la cible d'évaluation;
   f) toutes les exigences de sécurité sont rendues publiques. Les notes d'application peuvent donner des informations sur la manière dont les exigences fonctionnelles des critères communs visés à l'article 3 ont été utilisées pour comprendre la cible de sécurité;
   g) le résumé de la cible d'évaluation comprend toutes les fonctions de sécurité de la cible d'évaluation, mais les informations exclusives supplémentaires peuvent être retirées;
   h) les références aux profils de protection appliqués à la cible d'évaluation sont incluses;
   i) la justification peut être assainie pour supprimer les informations exclusives.

4. Même si la cible de sécurité assainie n'est pas formellement évaluée conformément aux normes d'évaluation visées à l'article 3, l'organisme de certification veille à ce qu'elle soit conforme à la cible de sécurité complète et évaluée, et fait référence à la cible de sécurité complète et assainie dans le rapport de certification.

ANNEXE VI

Portée de l'évaluation des pairs et composition de l'équipe d'évaluation par les pairs

VI.1 **Portée de l'évaluation par les pairs**

1. Les types d'évaluations par les pairs suivants sont couverts:

   a) Type 1: lorsqu'un organisme de certification exerce des activités de certification au niveau AVA_VAN.3;

   b) Type 2: lorsqu'un organisme de certification exerce des activités de certification liées à un domaine technique figurant sur la liste des documents de référence à l'annexe I;

   c) Type 3: lorsqu'un organisme de certification exerce des activités de certification supérieures au niveau AVA_VAN.3 en utilisant un profil de protection figurant sur la liste des documents de référence à l'annexe II ou III.

2. L'organisme de certification évalué par les pairs soumet la liste des produits TIC certifiés qui peuvent être candidats à l'examen par l'équipe d'évaluation par les pairs, conformément aux règles suivantes:

   a) les produits candidats couvrent le champ d'application technique de l'autorisation de l'organisme de certification, dont au moins deux évaluations de produits différents au niveau d'assurance «élevé» seront analysées dans le cadre de l'évaluation par les pairs, et un profil de protection si l'organisme de certification a délivré un certificat au niveau d'assurance «élevé»;

   b) pour une évaluation par les pairs de type 2, l'organisme de certification soumet au moins un produit par domaine technique et par CESTI concerné;

   c) pour une évaluation par les pairs de type 3, au moins un produit candidat est évalué conformément à un profil de protection applicable et pertinent.

VI.2 **Équipe d'évaluation par les pairs**

1. L'équipe d'évaluation est composée d'au moins deux experts, chacun choisi dans un organisme de certification d'un État membre différent qui délivre des certificats de niveau d'assurance «élevé». Les experts doivent démontrer qu'ils ont les compétences nécessaires en ce qui concerne les normes visées à l'article 3 et les documents de référence relevant du champ d'application de l'évaluation par les pairs.

2. Dans le cas d'une délégation de la délivrance de certificat ou d'une approbation préalable des certificats visée à l'article 56, paragraphe 6, du règlement (UE) 2019/881, un expert de l'autorité nationale de certification de cybersécurité liée à l'organisme de certification concerné intègre en outre l'équipe d'experts sélectionnés conformément au paragraphe 1 de la présente section.

3. Pour une évaluation par les pairs de type 2, les membres de l'équipe sont sélectionnés parmi les organismes de certification autorisés pour le domaine technique concerné.

4. Chaque membre de l'équipe d'évaluation a au moins deux ans d'expérience en matière de certification au sein d'un organisme de certification.

5. Pour une évaluation par les pairs de type 2 ou 3, chaque membre de l'équipe d'évaluation a au moins deux ans d'expérience en matière de certification dans le domaine technique ou le profil de protection concerné; chaque membre peut en outre démontrer son expertise en matière d'autorisation de CESTI et sa participation à ce type de procédure d'autorisation.

6. L'autorité nationale de certification de cybersécurité qui contrôle et supervise l'organisme de certification évalué par les pairs et au moins une autorité nationale de certification de cybersécurité dont l'organisme de certification n'est pas soumis à l'évaluation par les pairs participent à l'évaluation par les pairs en tant qu'observateurs. L'ENISA aussi peut participer à l'évaluation par les pairs en qualité d'observateur.

7. La composition de l'équipe d'évaluation par les pairs est présentée à l'organisme de certification évalué par les pairs. Dans des cas justifiés, ce dernier peut contester la composition de l'équipe d'évaluation par les pairs et demander sa révision.

ANNEXE VII

Contenu d'un certificat EUCC

Un certificat EUCC contient au moins:

a) un identifiant unique établi par l'organisme de certification délivrant le certificat;

b) des informations relatives au produit TIC ou au profil de protection certifié et au titulaire du certificat, notamment:

1) le nom du produit TIC ou du profil de protection et, le cas échéant, de la cible d'évaluation;

2) le type de produit TIC ou de profil de protection et, le cas échéant, de la cible d'évaluation;

3) la version du produit TIC ou du profil de protection;

4) le nom, l'adresse et les coordonnées du titulaire du certificat;

5) le lien vers le site web du titulaire du certificat contenant les informations supplémentaires en matière de cybersécurité visées à l'article 55 du règlement (UE) 2019/881;

c) les informations relatives à l'évaluation et à la certification du produit TIC ou du profil de protection, y compris:

1) le nom, l'adresse et les coordonnées de l'organisme de certification qui a délivré le certificat;

2) s'il est différent de l'organisme de certification, le nom du CESTI qui a réalisé l'évaluation;

3) le nom de l'autorité nationale de certification de cybersécurité responsable;

4) une référence au présent règlement;

5) une référence au rapport de certification associé au certificat visé à l'annexe V;

6) le niveau d'assurance applicable conformément à l'article 4;

7) une référence à la version des normes utilisées pour l'évaluation, visée à l'article 3;

8) l'identification du niveau d'assurance ou du paquet d'assurance spécifié dans les normes visées à l'article 3 et conformément à l'annexe VIII, y compris les composantes d'assurance utilisées et le niveau AVA_VAN couvert;

9) le cas échéant, la référence à un ou plusieurs profils de protection auxquels le produit TIC ou le profil de protection est conforme;

10) la date de délivrance;

11) la durée de validité du certificat;

d) la marque et l'étiquette associées au certificat conformément à l'article 11.

ANNEXE VIII

Déclaration du paquet d'assurance

1. Contrairement aux définitions des critères communs, une augmentation:

a) n'est pas désignée par l'abréviation «+»;

b) est détaillée dans la liste complète des composants concernés;

c) est décrite en détail dans le rapport de certification.

2. Le niveau d'assurance confirmé dans un certificat EUCC peut être complété par le niveau d'assurance de l'évaluation tel que spécifié à l'article 3 du présent règlement.

3. Si le niveau d'assurance confirmé dans un certificat EUCC ne fait pas référence à une augmentation, le certificat EUCC indique l'un des paquets suivants:

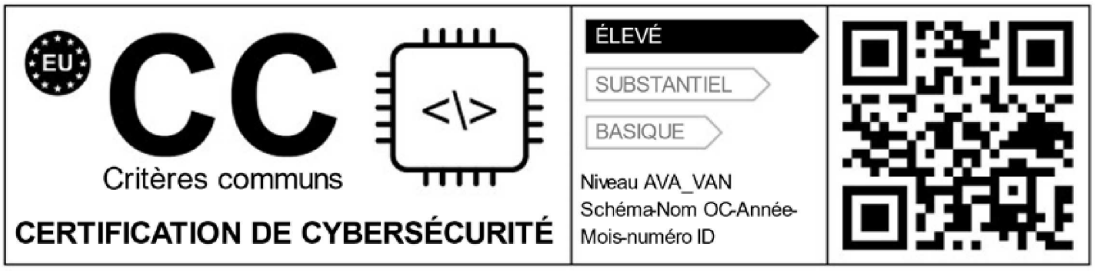
a) «le paquet d'assurance spécifique»;

b) «le paquet d'assurance conforme à un profil de protection» en cas de référence à un profil de protection sans niveau d'assurance de l'évaluation.

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 dans le dessin ci-dessus sont respectées.

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