Journal officiel
de l'Union européenne

FR
Série L

2025/2392

1.12.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/2392 DE LA COMMISSION

du 28 novembre 2025

relative à la description technique des catégories de produits importants et critiques comportant des éléments numériques, conformément au règlement (UE) 2024/2847 du Parlement européen et du Conseil

(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) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) nº 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience) ([1]), et en particulier son article 7, paragraphe 4, deuxième alinéa,

considérant ce qui suit:

(1) Le règlement (UE) 2024/2847 établit des règles relatives à la cybersécurité des produits comportant des éléments numériques. En particulier, l'annexe III dudit règlement définit des catégories de produits importants comportant des éléments numériques qui, lorsqu'ils sont mis sur le marché, sont soumis à des procédures d'évaluation de la conformité plus strictes que celles applicables aux autres produits comportant des éléments numériques. L'annexe IV du règlement (UE) 2024/2847 définit les catégories de produits critiques comportant des éléments numériques pour lesquels les fabricants pourraient être tenus d'obtenir un certificat de cybersécurité européen dans le cadre d'un schéma européen de certification de cybersécurité conformément au règlement (UE) 2019/881 du Parlement européen et du Conseil ([2]) ou qui seraient soumis à une évaluation obligatoire de la conformité par un tiers, lors de leur mise sur le marché.

(2) Conformément à l'article 7, paragraphe 1, et à l'article 8, paragraphe 1, du règlement (UE) 2024/2847, la fonctionnalité de base d'un produit comportant des éléments numériques détermine si ce produit correspond à la description technique d'une catégorie de produits importants ou critiques comportant des éléments numériques et, partant, s'il est soumis aux procédures d'évaluation de la conformité applicables.

(3) Lors de la mise au point d'un produit comportant des éléments numériques, et afin d'assurer l'ensemble de fonctionnalités visées, les fabricants intègrent généralement dans leurs propres produits comportant des éléments numériques d'autres composants qui sont également des produits comportant des éléments numériques et qui peuvent correspondre à la description technique d'une catégorie de produits importants ou critiques. En vertu du règlement (UE) 2024/2847, un produit comportant des éléments numériques est soumis aux procédures d'évaluation de la conformité applicables aux produits importants ou critiques comportant des éléments numérique s, si ce produit dans son ensemble est un produit important ou critique conformément aux annexes III et IV dudit règlement. Par exemple, l'intégration d'un navigateur intégré en tant que composant d'une application d'information destinée à être utilisée dans des smartphones ne rend pas en soi cette application soumise à la procédure d'évaluation de la conformité applicable aux produits comportant des éléments numériques qui ont la fonctionnalité principale de «navigateurs autonomes et intégrés». Néanmoins, conformément au règlement (UE) 2024/2847, le fabricant doit veiller à ce que le produit comportant des éléments numériques dans son ensemble satisfasse aux exigences essentielles de cybersécurité. Par conséquent, le fabricant doit évaluer la sécurité de l'ensemble du produit, en tenant compte, le cas échéant, de la sécurité des composants ou fonctionnalités qui y sont intégrés. Par exemple, pour que le fabricant d'une application d'actualités démontre que son produit comportant des éléments numériques est conforme au règlement (UE) 2024/2847, il doit démontrer que cette application d'actualités dans son ensemble satisfait aux exigences applicables, en tenant compte, le cas échéant, de la sécurité du navigateur intégré qui est intégré dans son application.

([1]) JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

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

(4) Le fait qu'un produit comportant des éléments numériques remplisse des fonctions autres que celles détaillées dans les descriptions techniques énoncées dans le présent règlement ou en complément de celles-ci ne signifie pas en soi que le produit comportant des éléments numériques n'a pas la fonctionnalité de base d'une catégorie de produits figurant aux annexes III et IV du règlement (UE) 2024/2847. Par exemple, les produits comportant des éléments numériques qui ont la fonctionnalité de base des «systèmes d'exploitation» comprennent souvent des logiciels qui remplissent des fonctions auxiliaires qui ne figurent pas dans la description technique de cette catégorie de produits, telles que des calculateurs ou des éditeurs graphiques simples. Les produits comportant des éléments numériques comprennent souvent également des composants qui ont la fonctionnalité d'un autre produit important ou critique comportant des éléments numériques, tels qu'un système d'exploitation intégrant une fonctionnalité de navigateur ou un routeur intégrant une fonctionnalité de pare-feu. Cela ne signifie toutefois pas en soi que ces produits comportant des éléments numériques n'ont pas la fonctionnalité de base des «systèmes d'exploitation» ou des «routeurs, modems destinés à la connexion à l'internet et commutateurs», respectivement.

(5) D'autre part, un produit comportant des éléments numériques qui est capable de remplir les fonctions d'une catégorie de produits figurant aux annexes III et IV du règlement (UE) 2024/2847 mais dont la fonctionnalité de base est elle-même différente de celle d'une telle catégorie de produits ne doit pas être considéré comme correspondant à la description technique de cette catégorie de produits. Par exemple, un logiciel SOAR (orchestration, automatisation et réponse en matière de sécurité) a souvent la capacité d'exécuter les fonctions de produits comportant des éléments numériques dans la catégorie des «systèmes de gestion des informations et des événements de sécurité (SIEM)», c'est-à-dire de recueillir des données, de les analyser et de les présenter comme des informations exploitables à des fins de sécurité. Toutefois, étant donné que sa fonctionnalité principale n'est pas celle d'un SIEM, un logiciel SOAR ne doit généralement pas être considéré comme correspondant à la description technique des «systèmes de gestion des informations et des événements de sécurité (SIEM)». De même, un smartphone intègre habituellement des composants qui remplissent les fonctions de plusieurs catégories de produits énoncées aux annexes III e IV du règlement (UE) 2024/2847, telles qu'un système d'exploitation ou un gestionnaire de mot de passe intégré. Toutefois, étant donné que la fonctionnalité principale d'un smartphone n'est pas celle d'un système d'exploitation ou d'un gestionnaire de mot de passe, il ne doit généralement pas être considéré comme correspondant à la description technique de ces catégories de produits.

(6) Conformément à l'article 13, paragraphes 2 et 3 du règlement (UE) 2024/2847, les fabricants de produits comportant des éléments numériques doivent mettre en œuvre les exigences essentielles de cybersécurité énoncées à l'annexe I, partie I, du règlement (UE) 2024/2847 d'une manière proportionnée aux risques du produit comportant des éléments numériques, en fonction de la destination et de l'utilisation raisonnablement prévisible, ainsi que des conditions d'utilisation du produit comportant des éléments numériques, compte tenu de la durée d'utilisation prévue du produit. Conformément à l'article 13, paragraphes 2 et 3 dudit règlement, et indépendamment de la question de savoir si le produit comportant des éléments numériques est considéré comme un produit important ou critique comportant des éléments numériques, les fabricants doivent procéder à une évaluation complète des risques de cybersécurité et indiquer comment les exigences essentielles de cybersécurité sont mises en œuvre sur la base de l'évaluation des risques, y compris les essais et l'assurance y afférents. Lorsque la fonctionnalité de base de leur produit comportant des éléments numériques correspond à la description technique d'un produit comportant des éléments numériques importants ou critiques, les fabricants doivent démontrer la conformité selon les procédures spécifiques d'évaluation de la conformité établies par l'article 32, paragraphes 2, 3, 4 et 5, du règlement (UE) 2024/2847.

(7) Le présent règlement comprend des exemples de produits comportant des éléments numériques dont la fonctionnalité de base correspond à la description technique de certains produits importants ou critiques comportant des éléments numériques. Ces exemples ne sont fournis qu'à titre indicatif et ne constituent pas une liste exhaustive.

(8) Afin d'apporter une sécurité juridique aux fabricants, il convient de distinguer les catégories de produits comportant des éléments numériques qui sont des microprocesseurs inviolables, des microcontrôleurs inviolables et des cartes à puce et dispositifs similaires, y compris des éléments sécurisés, en fonction du niveau de résistance à l'exploitabilité potentielle des défauts ou faiblesses pour lequel ils ont été conçus. Le niveau AVA_VAN est un moyen largement utilisé et normalisé d'exprimer un tel niveau de résistance. Les niveaux AVA_VAN sont définis dans les critères communs et les normes de la méthodologie commune d'évaluation accessibles au public, qui sont à la base de cadres de certification existants largement adoptés sur le marché, tels que le règlement d'exécution (UE) 2024/482 de la

Commission ([3]). Le règlement d'exécution (UE) 2024/482 établit un schéma européen de certification de cybersécurité qui peut être utilisé pour certifier un produit à un niveau d'assurance spécifique. S'appuyant sur les pratiques mondiales, le règlement d'exécution (UE) 2024/482 prévoit la possibilité de délivrer des certificats pour des versions plus anciennes des normes jusqu'à la fin de 2027. De ce fait, dans le contexte du règlement (UE) 2024/2847, il est approprié de permettre l'expression de niveaux AVA_VAN en référence à la version la plus récente ou à des versions plus anciennes de ces normes.

(9) Les mesures prévues par le présent règlement sont conformes à l'avis du comité institué par l'article 62, paragraphe 1, du règlement (UE) 2024/2847,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Définitions

Aux fins du présent règlement, on entend par:

1) «critères communs»: les critères communs d'évaluation de la sécurité des technologies de l'information définis à l'article 2, paragraphe 1, du règlement d'exécution (UE) 2024/482 ou définis dans les normes visées à l'article 3, paragraphe 2, points a) et b), dudit règlement d'exécution;

2) «méthode d'évaluation commune»: la méthode commune pour l'évaluation de la sécurité des technologies de l'information telle que définie à l'article 2, paragraphe 2, du règlement d'exécution (UE) 2024/482 ou définie dans les normes visées à l'article 3, paragraphe 2, points c) et d), dudit règlement d'exécution.

Article 2

1. La description technique des catégories de produits comportant des éléments numériques relevant des classes I et II énumérées à l'annexe III du règlement (UE) 2024/2847 est celle figurant à l'annexe I du présent règlement.

2. La description technique des catégories de produits comportant des éléments numériques énumérées à l'annexe IV du règlement (UE) 2024/2847 est celle figurant à l'annexe II du présent règlement.

Article 3

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

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

Fait à Bruxelles, le 28 novembre 2025.

Par la Commission
La présidente
Ursula VON DER LEYEN

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

ANNEXE I

PRODUITS IMPORTANTS COMPORTANT DES ÉLÉMENTS NUMÉRIQUES

Catégorie I

Catégorie de produits	Description technique
1. Systèmes de gestion des identités et logiciels et dispositifs de gestion des accès privilégiés, dont lecteurs d'authentification et de contrôle d'accès et lecteurs biométriques	Les systèmes de gestion de l'identité sont des produits comportant des éléments numériques qui prévoient des mécanismes d'authentification ou d'autorisation et qui peuvent également prévoir des mécanismes de gestion tout au long du cycle de vie des identifiants des personnes physiques, des personnes morales, des dispositifs ou des systèmes, tels que l'enregistrement de l'identité, la fourniture, la maintenance et la radiation de l'identité. Ces systèmes comprennent les systèmes de gestion des accès qui contrôlent l'accès des personnes physiques, des personnes morales, des dispositifs ou des systèmes aux ressources numériques ou aux lieux physiques. Le logiciel de gestion des accès privilégiés est un système de gestion des accès qui contrôle et surveille les droits d'accès aux systèmes informatiques ou opérationnels et aux informations sensibles au sein d'une organisation, y compris les systèmes appliquant des politiques de contrôle d'accès différenciées pour les utilisateurs privilégiés. Cette catégorie comprend, sans s'y limiter, les lecteurs d'authentification et de contrôle d'accès, les lecteurs biométriques, les logiciels d'authentification unique, les logiciels de gestion des identités fédérés, les logiciels de mot de passe à usage unique, les dispositifs d'authentification matériels tels que les générateurs de numéros d'authentification de transaction (TAN), les logiciels d'authentification et les logiciels d'authentification multifactorielle.
2. Navigateurs autonomes et intégrés	Les produits logiciels comportant des éléments numériques qui permettent aux utilisateurs finaux d'accéder aux contenus et services web hébergés sur des serveurs connectés à des réseaux tels que l'internet, de les afficher ou les utiliser et d'interagir avec eux. Ils comprennent généralement un moteur de navigateur pour l'interprétation et l'affichage de contenus écrits dans un langage de balisage (par exemple, HTML), un support pour les protocoles web (par exemple HTTP, HTTPS), la capacité d'exécuter des scripts et de gérer les entrées des utilisateurs ainsi que le stockage de données temporaires ou persistantes provenant de sites web (cookies). Cette catégorie comprend, sans s'y limiter, les applications autonomes qui remplissent les fonctions des navigateurs, les navigateurs intégrés destinés à être intégrés dans un autre système ou application, ainsi que les navigateurs intégrant des agents d'IA.
3. Gestionnaires de mots de passe	Les produits comportant des éléments numériques qui stockent des mots de passe localement sur un appareil ou sur un serveur à distance, y compris des activités telles que la génération de mots de passe et le partage de mots de passe ainsi que l'intégration avec des applications locales ou tierces pour l'utilisation de mots de passe. Cette catégorie comprend, sans s'y limiter, les gestionnaires de mots de passe locaux, les gestionnaires de mots de passe fournis sous forme d'extensions de navigateurs, les gestionnaires de mot de passe d'entreprise ainsi que les gestionnaires de mots de passe basés sur le matériel.

Catégorie de produits	Description technique
4. Logiciels qui recherchent, suppriment ou mettent en quarantaine des logiciels malveillants	Les logiciels comportant des éléments numériques, généralement appelés antivirus ou antilogiciels malveillants, qui détectent ou recherchent des logiciels malveillants ou des codes sur des dispositifs, ou retirent ou mettent en quarantaine ces logiciels ou codes, afin de préserver l'intégrité, la confidentialité ou la disponibilité de ces dispositifs. Dans le contexte de cette catégorie de produits, on entend par «logiciels malveillants» les logiciels contenant des caractéristiques ou des capacités malveillantes qui peuvent causer un préjudice direct ou indirect à l'utilisateur et/ou au système informatique, tels que les virus, les vers, les rançongiciels, les logiciels espions et les chevaux de Troie. Cette catégorie comprend, sans s'y limiter, les logiciels qui détectent ou recherchent des logiciels malveillants en temps réel ou manuellement, les disques de détection des outils de dissimulation d'activité (rootkit) et de sauvetage avec la fonctionnalité essentielle de recherche, de retrait ou de mise en quarantaine de logiciels malveillants.
5. Produits comportant des éléments numériques avec la fonction de réseau privé virtuel (VPN)	Les produits comportant des éléments numériques qui établissent un tunnel logique crypté construit à partir des ressources du système d'un réseau physique ou virtuel. Cette catégorie comprend, sans s'y limiter, les clients de réseaux privés virtuels, les serveurs de réseaux privés virtuels et les passerelles de réseaux privés virtuels.
6. Systèmes de gestion de la qualité	Les produits comportant des éléments numériques qui gèrent des éléments de réseau connectés, tels que les serveurs, les routeurs, les commutateurs, les postes de travail, les imprimantes ou les appareils mobiles, en les surveillant et en contrôlant leur fonctionnement et leur configuration de réseau. Cette catégorie comprend, sans s'y limiter, les systèmes de gestion de bout en bout et les systèmes de gestion de configuration dédiés, tels que les contrôleurs pour la mise en réseau définie par logiciel.
7. Systèmes de gestion des informations et des événements de sécurité (SIEM)	Les produits comportant des éléments numériques qui collectent des données provenant de sources multiples, analysent et mettent en corrélation ces données et les présentent comme des informations exploitables à des fins liées à la sécurité, telles que la détection des menaces et des incidents, l'analyse médico-légale ou la conformité.
8. Gestionnaires de démarrage	Les logiciels comportant des éléments numériques qui gèrent le processus de démarrage initial du système après la mise en puissance/le redémarrage en initialisant le matériel, en chargeant ou en transférant la commande dans l'environnement du système d'exploitation ou les ressources du système, et en sélectionnant des options de démarrage. Cette catégorie comprend, sans s'y limiter, le micrologiciel UEFI, les chargeurs d'amorçage en une ou plusieurs étapes.
9. Infrastructure à clé publique et logiciels d'émission de certificats numériques	Les produits comportant des éléments numériques utilisés dans le cadre d'une infrastructure à clé publique (ICP) qui gèrent la validation, la création, la délivrance, la distribution, la publication du statut, le renouvellement ou la révocation de certificats numériques, ou la production, le stockage, le séquestre, l'échange, la destruction ou la rotation de clés cryptographiques associées à ces certificats numériques. Cette catégorie comprend, sans s'y limiter, les systèmes de gestion des clés, les systèmes de gestion des certificats numériques, les services OSCP et les solutions d'ICP tout-en-un.

Catégorie de produits	Description technique
10. Interfaces réseau physiques et virtuelles	Les interfaces de réseau physiques sont des produits comportant des éléments numériques qui connectent directement un appareil à un réseau au moyen d'une interface de programmation d'application (API) fournie par les pilotes de l'interface, qui fonctionnent généralement à la couche de liaison de données, et qui présentent des adaptateurs matériels aux supports de transmission avec le micrologiciel correspondant, qui fonctionnent généralement à la couche de liaison physique et de liaison de données. Les interfaces de réseau virtuelles sont des produits comportant des éléments numériques qui connectent directement ou indirectement un appareil à un réseau au moyen d'une API émulant celle des pilotes d'interfaces de réseau physiques, qui fonctionnent généralement à la couche de liaison de données. Cette catégorie comprend, sans s'y limiter, les cartes d'interface réseau filaire et sans fil, les contrôleurs et adaptateurs, tels que Wi-Fi, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee ou Fieldbus, ainsi que les produits autonomes purement virtuels, tels que les cartes d'interface réseau virtuel, les interfaces réseau de conteneurs et les interfaces VPN.
11. Systèmes d'exploitation	Les produits logiciels comportant des éléments numériques qui fournissent une interface abstraite avec le matériel sous-jacent et contrôlent l'exécution des logiciels, et qui peuvent fournir des services tels que la gestion et la configuration des ressources informatiques, la programmation, le contrôle entrée-sortie, la gestion des données et la fourniture d'une interface par l'intermédiaire de laquelle les applications interagissent avec les ressources du système et les périphériques. Cette catégorie comprend, sans s'y limiter, les systèmes d'exploitation en temps réel, les systèmes d'exploitation à usage général et les systèmes d'exploitation à usage spécial.
12. Routeurs, modems destinés à la connexion à l'internet et commutateurs	Les routeurs sont des produits comportant des éléments numériques qui établissent et contrôlent le flux de données entre les différents réseaux en sélectionnant des chemins ou des itinéraires à l'aide de mécanismes et d'algorithmes de protocole de routage, qui fonctionnent généralement à la couche réseau. Cette catégorie comprend, sans s'y limiter, les routeurs filaires et sans fil, les routeurs virtuels et les routeurs avec ou sans modems.
	Les modems destinés à la connexion à l'internet sont des produits matériels comportant des éléments numériques qui utilisent des techniques de modulation numérique et de démodulation pour convertir les signaux analogiques depuis et vers les signaux numériques pour la communication IP. Cette catégorie comprend, sans s'y limiter, les modems à fibre optique, les modems de ligne d'abonné numérique (DSL), les modems par câble (DOCSIS), les modems satellites et les modems cellulaires.
	Les commutateurs sont des produits comportant des éléments numériques qui assurent la connectivité entre les dispositifs en réseau au moyen de mécanismes de transmission de paquets et qui disposent d'un plan de gestion (*management plane*), généralement mis en œuvre à la liaison de données ou à la couche réseau. Cette catégorie comprend, sans s'y limiter, les commutateurs gérés, les commutateurs intelligents, les commutateurs multicouches, les interrupteurs virtuels de sécurité, les commutateurs programmables pour la mise en réseau définie par logiciel et les ponts tels que les points d'accès sans fil.

Catégorie de produits	Description technique
13. Microprocesseurs dotés de fonctionnalités liées à la sécurité	Les produits comportant des éléments numériques qui sont des circuits intégrés assurant des fonctions de traitement centrales reposant sur une mémoire externe et des périphériques, y compris des microcodes et d'autres micrologiciels de faible niveau. Ils fournissent en outre des fonctionnalités liées à la sécurité, telles que le cryptage, l'authentification, le stockage sécurisé des clés, la génération aléatoire de numéros, l'environnement d'exécution de confiance ou d'autres mécanismes de protection fondés sur le matériel, qui visent à sécuriser d'autres produits, réseaux ou services au-delà du microprocesseur lui-même, tels que la chaîne d'amorçage sécurisée, la virtualisation ou les interfaces de communication sécurisées.
14. Microcontrôleurs dotés de fonctionnalités liées à la sécurité	Les produits comportant des éléments numériques qui sont des circuits intégrés assurant des fonctions de traitement centrales intégrant une mémoire qui permet la programmabilité du microcontrôleur et habituellement d'autres périphériques, notamment des microcodes et d'autres micrologiciels de faible niveau. Ils fournissent en outre des fonctionnalités liées à la sécurité, telles que le cryptage, l'authentification, le stockage sécurisé des clés, la génération aléatoire de numéros, l'environnement d'exécution de confiance ou d'autres mécanismes de protection fondés sur le matériel, qui visent à sécuriser d'autres produits, réseaux ou services au-delà du microprocesseur lui-même, tels que la chaîne d'amorçage sécurisée, la virtualisation ou les interfaces de communication sécurisées.
15. Circuits intégrés spécifiques à l'application (ASIC) et réseaux de portes programmables (FPGA) dotés de fonctionnalités liées à la sécurité	Les circuits intégrés spécifiques à une application (ASIC) dotés de fonctionnalités liées à la sécurité sont des produits comportant des éléments numériques qui sont des circuits intégrés, entièrement ou partiellement personnalisés, conçus pour remplir une fonction spécifique ou mettre en œuvre une application spécifique, y compris le microcode et d'autres micrologiciels de faible niveau. Ils fournissent en outre des fonctionnalités liées à la sécurité, telles que le cryptage, l'authentification, le stockage sécurisé des clés, la génération aléatoire de numéros, l'environnement d'exécution de confiance ou d'autres mécanismes de protection fondés sur le matériel, qui visent à sécuriser d'autres produits, réseaux ou services au-delà du microprocesseur lui-même, tels que la chaîne d'amorçage sécurisée, la virtualisation ou les interfaces de communication sécurisées.
	Les réseaux de portes programmables in situ (FPGA) dotés de fonctionnalités liées à la sécurité sont des produits comportant des éléments numériques qui sont des circuits intégrés caractérisés par une matrice de blocs logiques configurables conçus pour être reprogrammables après leur fabrication afin de remplir une fonction spécifique ou de mettre en œuvre une application spécifique, y compris le microcode et d'autres micrologiciels de faible niveau. Ils fournissent en outre des fonctionnalités liées à la sécurité, telles que le cryptage, l'authentification, le stockage sécurisé des clés, la génération aléatoire de numéros, l'environnement d'exécution de confiance ou d'autres mécanismes de protection fondés sur le matériel, qui visent à sécuriser d'autres produits, réseaux ou services au-delà du FGPA lui-même, tels que la chaîne d'amorçage sécurisée, la virtualisation ou les interfaces de communication sécurisées.
16. Assistants virtuels polyvalents pour maison intelligente	Les produits comportant des éléments numériques qui communiquent sur l'internet public, que ce soit directement ou par l'intermédiaire d'autres équipements, qui traitent des demandes, des tâches ou des questions fondées sur le langage naturel, telles que des entrées audio ou écrites, et qui, sur la base de ces demandes, tâches ou questions, donnent accès à d'autres services ou contrôlent les fonctions des appareils connectés dans des environnements résidentiels. Cette catégorie comprend, sans s'y limiter, les haut-parleur intelligents dotés d'un assistant virtuel intégré et les assistants virtuels autonomes qui répondent à cette description.

Catégorie de produits	Description technique
17. Produits domestiques intelligents dotés de fonctionnalités de sécurité, notamment serrures, caméras de sécurité, systèmes de surveillance pour bébé et systèmes d'alarme	Les produits comportant des éléments numériques qui protègent la sécurité physique des consommateurs dans un environnement résidentiel et qui peuvent être contrôlés ou gérés à distance à partir d'autres systèmes, ainsi que le matériel et les logiciels qui contrôlent ces produits de manière centralisée. Cette catégorie comprend, sans s'y limiter, les dispositifs intelligents de verrouillage des portes, les systèmes de surveillance des bébés, les systèmes d'alarme et les caméras de sécurité à domicile.
18. Jouets connectés couverts par la directive 2009/48/CE du Parlement européen et du Conseil ([1]) qui présentent des caractéristiques sociales interactives (par exemple, parler ou filmer) ou qui possèdent des fonctions de localisation.	Les jouets connectés à l'internet qui présentent des caractéristiques sociales interactives sont des produits comportant des éléments numériques qui sont couverts par la directive 2009/48/CE, qui communiquent sur l'internet public, directement ou par l'intermédiaire de tout autre équipement, et qui disposent de technologies intégrées permettant la communication entrante et sortante, telles que le clavier, le microphone, le haut-parleur ou la caméra.
	Les jouets connectés à l'internet qui comportent des fonctionnalités de localisation sont des produits comportant des éléments numériques qui sont couverts par la directive 2009/48/CE, qui communiquent sur l'internet public, que ce soit directement ou par l'intermédiaire de tout autre équipement, et qui disposent de technologies permettant de suivre ou de déduire la localisation géographique du jouet ou de son utilisateur. Lorsque le jouet détecte simplement la proximité de l'utilisateur ou d'autres jouets au moyen de technologies de détection, le jouet ne doit pas être considéré comme ayant des caractéristiques de localisation.
19. Produits portables personnels destinés à être portés ou mis sur un corps humain à des fins de surveillance de la santé (suivi par exemple) et auxquels le règlement (UE) 2017/745 ([2]) ou (UE) 2017/746 ([3]) du Parlement européen et du Conseil ne s'applique pas, ou produits portables personnels destinés à être utilisés par et pour les enfants	Les produits portables personnels destinés à être portés ou placés sur le corps humain à des fins de surveillance de la santé sont des produits comportant des éléments numériques qui sont portés sur le corps directement ou par l'intermédiaire de vêtements ou d'accessoires et qui peuvent, de manière régulière ou continue, capter et traiter des informations, y compris des paramètres corporels, ayant trait à la santé de l'utilisateur, à l'exclusion des produits qui relèvent du champ d'application du règlement (UE) 2017/745 ou du règlement (UE) 2017/746. Cette catégorie comprend, sans s'y limiter, les dispositifs de suivi de la condition physique, les montres intelligentes, les bijoux intelligents, les vêtements intelligents et les vêtements de sport qui répondent à cette description.
	Les produits portables personnels destinés à être utilisés par et pour les enfants sont des produits comportant des éléments numériques qui peuvent être portés ou placés sur le corps, directement ou par l'intermédiaire de vêtements ou d'accessoires, de personnes de moins de 14 ans. Cette catégorie comprend, sans s'y limiter, les dispositifs portables de sécurité pour enfants.

([1]) Directive 2009/48/CE du Parlement européen et du Conseil du 18 juin 2009 relative à la sécurité des jouets (JO L 170 du 30.6.2009, p. 1, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) nº 178/2002 et le règlement (CE) nº 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE (JO L 117 du 5.5.2017, p. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj.

([3]) Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission (JO L 117 du 5.5.2017, p. 176, ELI: http://data.europa.eu/eli/reg/2017/746/oj.

Catégorie II

Catégorie de produits	Description technique
1. Hyperviseurs et systèmes d'exécution de conteneurs prenant en charge l'exécution virtualisée de systèmes d'exploitation et d'environnements similaires	Les hyperviseurs sont des produits logiciels comportant des éléments numériques qui extraient et/ou attribuent des ressources informatiques et permettent l'exécution, la gestion et l'orchestration de machines virtuelles qui sont logiquement séparées les unes des autres et/ou du matériel physique. Les hyperviseurs peuvent fonctionner directement sur du matériel (*bare metal*), au-dessus d'un système d'exploitation ou à l'intérieur d'une autre machine virtuelle (virtualisation imbriquée). Dans le contexte de cette catégorie de produits, une machine virtuelle est une séparation logique définie par logiciel d'un environnement informatique, qui comprend un ensemble virtualisé de ressources matérielles (par exemple, CPU, mémoire, stockage, interfaces réseau) et qui héberge généralement son propre système d'exploitation. Cette catégorie comprend, sans s'y limiter, les hyperviseurs de type 1 (*bare metal*), les hyperviseurs de type 2 (hébergés sur un système d'exploitation) et les hyperviseurs hybrides.
	Les systèmes d'exécution de conteneurs sont des produits logiciels comportant des éléments numériques qui gèrent l'exécution et le cycle de vie de conteneurs fonctionnant sur un seul système d'exploitation hôte en tant que processus isolés, allouant des ressources et permettant la gestion et l'orchestration de conteneurs individuels. Dans le contexte de cette catégorie de produits, un conteneur est un environnement d'exécution fondé sur des logiciels qui intègre un ou plusieurs composants logiciels et leurs dépendances dans un seul et même emballage, ce qui lui permet de fonctionner de manière indépendante et cohérente.
2. Pare-feu, systèmes de détection et de prévention des intrusions	Les pare-feu sont des produits comportant des éléments numériques qui protègent un réseau ou un système connecté contre tout accès non autorisé en surveillant et en limitant le trafic de communication de données à destination et en provenance de ce réseau. Cette catégorie comprend, sans s'y limiter, les pare-feu de réseau et les pare-feu d'application tels que les pare-feu pour applications web ou les filtres et les passerelles anti-spam.
	Les systèmes de détection des intrusions sont des produits comportant des éléments numériques qui surveillent le trafic une fois qu'il est entré dans l'environnement de réseau et détectent ou constatent qu'une intrusion a été tentée, se produit ou s'est produite sur un réseau ou un système connecté. Cette catégorie comprend, sans s'y limiter, les systèmes de détection des intrusions basés sur le réseau et les systèmes de détection des intrusions basés sur l'hôte.
	Les systèmes de prévention des intrusions sont des produits comportant des éléments numériques composés d'un système de détection des intrusions qui répond activement à une intrusion dans un réseau ou un système connecté. Cette catégorie comprend, sans s'y limiter, les systèmes de prévention des intrusions basés sur le réseau et les systèmes de prévention des intrusions basés sur l'hôte.

Catégorie de produits	Description technique
3. Microprocesseurs résistants aux manipulations	Les produits comportant des éléments numériques qui sont des microprocesseurs dotés de fonctionnalités liées à la sécurité visés dans le tableau «Classe I», point 13, de la présente annexe, notamment les preuves de manipulation ou la résistance/réponse aux manipulations, et qui sont en outre conçus pour assurer la protection AVA_VAN niveau 2 ou 3, comme indiqué dans les critères communs et la méthodologie d'évaluation commune.
4. Microcontrôleurs résistants aux manipulations	Les produits comportant des éléments numériques qui sont des microprocesseurs dotés de fonctionnalités liées à la sécurité visés dans le tableau «Classe I», point 14, de la présente annexe, notamment les preuves de manipulation ou la résistance/réponse aux manipulations, et qui sont en outre conçus pour assurer la protection AVA_VAN niveau 2 ou 3, comme indiqué dans les critères communs et la méthodologie d'évaluation commune.

ANNEXE II

PRODUITS CRITIQUES COMPORTANT DES ÉLÉMENTS NUMÉRIQUES

Catégorie de produits	Description technique
1. Dispositifs matériels avec boîtier de sécurité	Les produits matériels comportant des éléments numériques qui stockent, traitent ou gèrent des données sensibles en toute sécurité ou effectuent des opérations cryptographiques, et qui consistent en plusieurs composants discrets, comprenant une enveloppe physique matérielle fournissant en cas de manipulation des preuves, une résistance ou une réaction, contre-mesures face aux attaques physiques. Cette catégorie comprend, sans s'y limiter, les terminaux de paiement physiques, les modules de sécurité matériels qui génèrent et gèrent des éléments cryptographiques et les tachygraphes qui répondent à la description ci-dessus.
2. «Passerelles pour compteur intelligent» au sein des systèmes intelligents de mesure tels que définis à l'article 2, point 23), de la directive (UE) 2019/944 du Parlement européen et du Conseil [1] et autres dispositifs à des fins de sécurité avancées, y compris pour un traitement cryptographique sécurisé	Les passerelles des compteurs intelligents sont des produits comportant des éléments numériques qui contrôlent la communication entre les composants des systèmes intelligents de mesure ou connectés à ceux-ci, tels que définis à l'article 2, paragraphe 23, de la directive (UE) 2019/944, et les tiers autorisés, tels que les fournisseurs de services d'utilité publique. Les passerelles des compteurs intelligents collectent, traitent et stockent des données de compteurs ou des données à caractère personnel, protègent les données et les flux d'informations en répondant à des besoins cryptographiques spécifiques, tels que le cryptage et le décryptage de données, intègrent des fonctionnalités de pare-feu et fournissent les moyens de contrôler d'autres dispositifs. Cette catégorie comprend, sans s'y limiter, les passerelles de compteurs intelligents liées aux systèmes intelligents de mesure de l'électricité tels que définis à l'article 2, paragraphe 23, de la directive (UE) 2019/944. Elle peut également inclure des passerelles de compteur intelligent utilisées dans d'autres systèmes intelligents de mesure de la consommation d'autres sources d'énergie telles que le gaz ou la chaleur, à condition que la passerelle réponde à cette description.
3. Cartes à puce ou dispositifs similaires, y compris éléments sécurisés	Les éléments sécurisés sont des microcontrôleurs ou des microprocesseurs dotés de fonctionnalités liées à la sécurité, notamment les preuves de manipulation ou la résistance/réponse aux manipulations. Ils stockent, traitent ou gèrent généralement des opérations cryptographiques ou des données sensibles, telles que des identifiants d'identité ou des identifiants de paiement. Les éléments sécurisés sont conçus pour assurer une protection d'au moins AVA_VAN.4, comme indiqué dans les critères communs ou la méthodologie d'évaluation commune. Ils peuvent être de silicium discret ou être intégrés dans des systèmes sur puce (SoC). Les éléments sécurisés peuvent intégrer un environnement d'application ou un système d'exploitation et peuvent comprendre une ou plusieurs applications. Cette catégorie comprend, sans s'y limiter, les modules de plateforme de confiance et les cartes à circuit intégré universelles embarquées (UICC).
	Les cartes à puce ou dispositifs similaires sont des éléments sécurisés intégrés dans un matériau porteur, tels que le plastique ou le bois, sous la forme d'une carte, ou des éléments sécurisés intégrés dans des matériaux porteurs prenant d'autres formes. Cette catégorie comprend, sans s'y limiter, les documents d'identité et de voyage, les cartes de signature qualifiées, les cartes à circuit intégré universelle embarquées (UICC) remplaçables, les cartes de paiement physiques, les cartes d'accès physiques, les cartes tachygraphiques numériques ou les bandes de poignet comportant des éléments intégrés sécurisés pour les paiements.

[1] Directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et modifiant la directive 2012/27/UE (JO L 158 du 14.6.2019, p. 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).