Journal officiel
de l'Union européenne

FR
Série L

2024/2981

4.12.2024

RÈGLEMENT D'EXÉCUTION (UE) 2024/2981 DE LA COMMISSION

du 28 novembre 2024

portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne la certification des portefeuilles européens d'identité numérique

LA COMMISSION EUROPÉENNE,

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

vu le règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE ([1]), et notamment son article 5 *quater*, paragraphe 6,

considérant ce qui suit:

(1) Conformément à l'article 5 *quater* du règlement (UE) nº 910/2014, la certification des portefeuilles européens d'identité numérique (ci-après les «portefeuilles») doit être effectuée conformément à des exigences fonctionnelles ainsi qu'à des exigences relatives à la cybersécurité et à la protection des données afin de garantir un niveau élevé de sécurité et de confiance dans les portefeuilles. Ces exigences en matière de certification doivent être harmonisées entre les États membres afin d'éviter la fragmentation du marché et de permettre la mise en place d'un cadre solide.

(2) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([2]) et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([3]) s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du présent règlement.

(3) La Commission évalue régulièrement de nouvelles technologies, pratiques, normes ou spécifications techniques. Afin d'atteindre le niveau d'harmonisation le plus élevé possible entre les États membres en ce qui concerne le développement et la certification des portefeuilles, les spécifications techniques énoncées dans le présent règlement s'appuient sur les travaux menés sur la base de la recommandation (UE) 2021/946 de la Commission du 3 juin 2021 concernant une boîte à outils commune de l'Union pour une approche coordonnée en vue d'un cadre européen relatif à une identité numérique ([4]), et en particulier sur l'architecture et le cadre de référence qui sont une composante de cette boîte à outils. Conformément au considérant 75 du règlement (UE) 2024/1183 du Parlement européen et du Conseil ([5]), la Commission devrait réexaminer et, si besoin est, mettre à jour le présent règlement d'exécution, afin de le maintenir en adéquation avec les évolutions au niveau mondial, l'architecture et le cadre de référence et de suivre les meilleures pratiques sur le marché intérieur.

(4) Afin d'attester la conformité aux exigences de cybersécurité figurant dans le cadre de certification, la certification des solutions de portefeuille devrait faire référence aux schémas européens de certification de cybersécurité établis en vertu du règlement (UE) 2019/881 du Parlement européen et du Conseil ([6]), lorsque ceux-ci sont disponibles et pertinents. En l'absence de tels schémas, ou lorsqu'ils ne couvrent que partiellement les exigences en matière de cybersécurité, le présent règlement définit les exigences d'ordre général applicables aux schémas nationaux de certification couvrant les exigences fonctionnelles, de cybersécurité et de protection des données.

([1]) JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).
([3]) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).
([4]) JO L 210 du 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.
([5]) Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique (JO L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).
([6]) 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).

(5) Conformément à l'article 5 *bis*, paragraphe 11, du règlement (UE) nº 910/2014, les portefeuilles doivent être certifiés au niveau de garantie élevé prévu par le règlement (UE) nº 910/2014, ainsi que par le règlement d'exécution (UE) 2015/1502 de la Commission ([7]). Ce niveau de garantie doit être atteint par l'intégralité de la solution de portefeuille. En vertu du présent règlement, certains composants de la solution de portefeuille peuvent être certifiés à un niveau de garantie inférieur, à condition que cela soit dûment justifié et sans préjudice du niveau de garantie élevé atteint par l'intégralité de la solution de portefeuille.

(6) Tous les schémas nationaux de certification devraient désigner un propriétaire de schéma qui sera responsable du développement et de la maintenance du schéma de certification. Le propriétaire du schéma peut être un organisme d'évaluation de la conformité, un organisme public ou une autorité publique, une association professionnelle, un groupe d'organismes d'évaluation de la conformité ou tout organisme approprié, et il peut être différent de l'organisme exploitant le schéma national de certification.

(7) L'objet de la certification devrait inclure les composants logiciels de la solution de portefeuille, tels que l'instance de portefeuille. L'application cryptographique sécurisée de portefeuille (WSCA), le dispositif cryptographique sécurisé de portefeuille (WSCD) et les plateformes sur lesquelles ces composants logiciels sont exécutés font partie de l'environnement d'exploitation mais ne devraient être inclus dans l'objet de la certification que s'ils sont fournis par la solution de portefeuille. Dans d'autres cas, et en particulier lorsque ces dispositifs et plateformes sont fournis par des utilisateurs finaux, les fournisseurs devraient établir des hypothèses relatives à l'environnement d'exploitation de la solution de portefeuille, notamment aux dispositifs et plateformes, et mettre en œuvre des mesures pour confirmer que ces hypothèses sont vérifiées dans la pratique. Afin d'assurer la protection des actifs critiques à l'aide du matériel et des logiciels de systèmes utilisés pour gérer et protéger les clés cryptographiques créées, stockées ou traitées par le dispositif cryptographique sécurisé de portefeuille, ce dernier doit satisfaire, au moyen d'une évaluation EAL4 et d'une analyse méthodique avancée des vulnérabilités de type AVA_VAN.5, à des exigences élevées en matière de certification telles que celles des normes internationales et des critères communs sur lesquels se fonde le schéma de certification de l'UE (EUCC) établi par le règlement d'exécution (UE) 2024/482 de la Commission ([8]), Ces normes de certification devraient être utilisées au plus tard lorsque la conformité des portefeuilles est certifiée selon un schéma européen de certification de cybersécurité adopté en vertu du règlement (UE) 2019/881.

(8) Les portefeuilles entièrement mobiles, sécurisés et conviviaux sont conditionnés par la disponibilité de solutions inviolables normalisées et certifiées, telles que des éléments sécurisés intégrés, des dispositifs externes tels que des cartes à puce ou des plateformes SIM intégrées dans des appareils mobiles. Il est important de veiller à ce que les moyens d'identification électronique nationaux et les portefeuilles aient accès en temps voulu aux éléments sécurisés intégrés, et de coordonner les efforts des États membres dans ce domaine. Par conséquent, il convient que le groupe de coopération européen en matière d'identité numérique institué en vertu de l'article 46 *sexies*, paragraphe 1, du règlement (UE) nº 910/2014 (ci-après dénommé «groupe de coopération») crée un sous-groupe chargé de cette tâche. En consultation avec les parties prenantes concernées, ce sous-groupe devrait convenir d'une feuille de route commune concernant l'accès aux éléments sécurisés intégrés, qui sera examinée par la Commission dans le cadre de son rapport relatif au réexamen de l'application du règlement (UE) nº 910/2014. Afin de faciliter l'adoption du portefeuille au niveau national, la Commission devrait en outre, en coopération avec les États membres, élaborer un manuel relatif aux cas d'usage à intégrer à l'architecture et au cadre de référence, et le mettre à jour en permanence.

(9) L'objet de la certification des schémas nationaux de certification devrait également inclure les processus utilisés pour fournir et faire fonctionner la solution de portefeuille, même si la définition ou l'exécution de ces processus est sous-traitée à des tiers. Il est permis d'utiliser les informations en matière de garantie comme éléments de preuve pour démontrer que les processus satisfont aux exigences des schémas, à condition de faire appel à une analyse des dépendances pour déterminer si ces informations sont suffisantes. Les informations en matière de garantie peuvent prendre des formes très diverses, telles que des rapports et des certificats de conformité, qui peuvent être privés, nationaux, européens ou internationaux, fondés sur des normes ou sur des spécifications techniques. L'objectif de l'analyse des dépendances consiste à évaluer la qualité des informations en matière de garantie disponibles concernant les composants d'un portefeuille.

([7]) Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) nº 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (JO L 235 du 9.9.2015, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([8]) 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/2024/482/oj).

(10) Conformément aux procédures établies à cette fin, le groupe de coopération devrait être en mesure de formuler des avis et des recommandations sur les projets de schémas nationaux de certification qui lui sont soumis. Ces schémas nationaux de certification devraient être propres à l'architecture du portefeuille et il devrait y avoir des profils spécifiques pour chaque architecture prise en charge.

(11) Afin de garantir une compréhension commune et une approche harmonisée de l'évaluation des risques les plus critiques susceptibles d'affecter la fourniture et le fonctionnement de portefeuilles, il convient d'établir un registre des risques et des menaces qui devraient être pris en considération lors de la conception de solutions de portefeuille, quelle que soit leur architecture. Lors de l'identification des risques qui devraient figurer dans le registre, il y a lieu de tenir compte des objectifs de cybersécurité décrits dans le règlement (UE) nº 910/2014, tels que la confidentialité, l'intégrité et la disponibilité de la solution de portefeuille, ainsi que la protection des données à caractère personnel et de la vie privée des utilisateurs. La prise en compte des risques et des menaces figurant dans ce registre devrait faire partie des exigences des schémas nationaux de certification. Il convient d'assurer la maintenance du registre des risques et de l'actualiser régulièrement en collaboration avec le groupe de coopération afin de rester en phase avec l'évolution constante du paysage des menaces.

(12) Lorsqu'ils établissent leurs schémas de certification, les propriétaires de schémas devraient procéder à une évaluation des risques afin d'affiner et de compléter la liste de risques et de menaces figurant dans le registre avec les risques et menaces propres à l'architecture ou à la mise en œuvre de la solution de portefeuille. L'évaluation des risques devrait examiner la manière dont les risques et menaces considérés peuvent être traités de manière appropriée. Les fournisseurs de portefeuille devraient compléter l'évaluation des risques du schéma afin d'identifier les risques et menaces propres à leur mise en œuvre de la solution et proposer des mesures de traitement appropriées pour évaluation par l'organisme de certification.

(13) Afin de démontrer qu'une architecture de solution de portefeuille satisfait aux exigences de sécurité applicables, chaque schéma ou profil propre à l'architecture devrait contenir au moins une description de l'architecture de la solution de portefeuille, une liste des exigences de sécurité applicables à l'architecture de la solution de portefeuille, un plan d'évaluation confirmant qu'une solution de portefeuille fondée sur cette architecture satisfait à ces exigences et une évaluation des risques. Les schémas nationaux de certification devraient exiger des fournisseurs de portefeuille qu'ils démontrent comment la conception de la solution de portefeuille qu'ils fournissent correspond à l'architecture de référence et détaille les contrôles de sécurité et les plans de validation de la solution de portefeuille considérée. Les schémas nationaux de certification devraient également définir une activité d'évaluation de la conformité permettant de vérifier que la conception du portefeuille reflète correctement l'architecture de référence du profil sélectionné. Les schémas nationaux de certification devraient être conformes aux exigences énoncées à l'article 51 du règlement (UE) 2019/881, à l'exception de ses points e) et f), relatifs à la journalisation.

(14) En ce qui concerne la certification des produits, il convient d'autoriser l'utilisation des certificats de conformité délivrés au titre du schéma de certification de cybersécurité de l'UE fondé sur des critères communs (EUCC) ainsi que des certificats de conformité délivrés au titre des schémas nationaux de certification dans le cadre de l'accord de reconnaissance mutuelle SOG-IS. En outre, pour des composants de produits moins sensibles, il y a lieu d'autoriser l'utilisation d'autres schémas nationaux de certification tels que ceux établis conformément à la norme CEN EN 17640 pour la méthode d'évaluation de la cybersécurité implémentée à l'aide d'une durée prédéfinie.

(15) Il convient d'utiliser le label de confiance du portefeuille européen d'identité numérique (ci-après le «label de confiance») pour indiquer de manière claire, simple et reconnaissable qu'un portefeuille a été fourni conformément au règlement (UE) nº 910/2014. Par conséquent, ce label devrait être considéré comme une marque de conformité pour les solutions de portefeuille certifiées au titre des schémas de certification nationaux. Les schémas nationaux de certification ne devraient pas définir d'autres marques de conformité.

(16) Afin de décourager la fraude, les schémas de certification nationaux devraient définir les mesures à prendre en cas de d'allégation frauduleuse de certification au titre du schéma.

(17) En vue de garantir une gestion efficiente des notifications de vulnérabilité, les fournisseurs de solutions de portefeuille et le schéma d'identification électronique dans le cadre duquel celles-ci sont fournies devraient définir et mettre en œuvre des processus d'évaluation de la gravité et de l'impact potentiel des vulnérabilités. Les schémas nationaux de certification devraient fixer un seuil à partir duquel l'organisme de certification doit être informé. Cette obligation d'information ne devrait pas porter atteinte aux critères établis par la législation en matière de protection des données et par les autorités des États membres chargées de la protection des données pour la notification des violations de données à caractère personnel. D'éventuelles synergies pourraient être établies entre la notification obligatoire de la violation ou de l'altération des solutions de portefeuille et la notification des violations de données à caractère personnel conformément au règlement (UE) 2016/679. L'évaluation d'un rapport d'analyse d'impact de la vulnérabilité par l'organisme de certification devrait être sans préjudice de l'évaluation, par une autorité chargée de la protection des données, d'une analyse d'impact relative à la protection des données conformément aux articles 35 et 36 du règlement (UE) 2016/679.

(18) Les fournisseurs de solutions de portefeuille et le schéma d'identification électronique dans le cadre duquel celles-ci sont fournies devraient communiquer au propriétaire du schéma les justifications éventuelles de toute exception à l'analyse des vulnérabilités requise pour l'évaluation du WSCD et de la WSCA, telle que prévue à l'annexe IV.

(19) L'annulation d'un certificat de conformité pourrait avoir de graves conséquences, telles que la révocation de toutes les unités de portefeuille déployées. Par conséquent, les organismes de certification ne devraient envisager l'annulation que si une vulnérabilité non corrigée est susceptible de porter atteinte de manière significative à la fiabilité de la solution de portefeuille ou à celle d'autres solutions de portefeuille.

(20) Il convient de mettre en place un processus spécifique de mise à jour des schémas nationaux de certification pour gérer la transition entre les versions successives des schémas, notamment quant aux mesures à prendre par le titulaire du certificat en ce qui concerne les évaluations à venir, la maintenance, la recertification et les évaluations spéciales.

(21) Pour faciliter la transparence, les fournisseurs de portefeuille devraient publier des informations de sécurité concernant leur solution de portefeuille.

(22) Lorsque des schémas nationaux de certification reposent sur des informations en matière de garantie provenant d'autres schémas ou sources de certification, il convient d'effectuer une analyse des dépendances afin de vérifier que les documents relatifs à la garantie, par exemple les rapports de garantie et les certificats de conformité, sont disponibles et adéquats pour les solutions de portefeuille et le schéma d'identification électronique dans le cadre duquel elles sont fournies. Cette analyse des dépendances devrait se fonder sur l'évaluation des risques des solutions de portefeuille et du schéma d'identification électronique dans le cadre duquel elles sont fournies. L'évaluation devrait déterminer si la documentation en matière de garantie disponible pour une solution de portefeuille donnée et le schéma d'identification électronique dans le cadre duquel celle-ci est fournie sont adéquats pour fournir une garantie correspondant au niveau d'évaluation ciblé. L'évaluation devrait également mettre à jour l'analyse des dépendances, ou la recommencer entièrement, le cas échéant.

(23) Les organismes de certification devraient délivrer des certificats de conformité dans le cadre des schémas nationaux de certification, accompagnés d'un rapport d'évaluation de la certification accessible au public, tel que visé à l'article 5 *quinquies*, paragraphe 2, point a), du règlement (UE) n° 910/2014. Il convient de mettre le rapport d'évaluation de la certification y afférent à la disposition du groupe de coopération.

(24) Les schémas nationaux de certification devraient prévoir une évaluation annuelle de surveillance afin de veiller au fonctionnement effectif des processus liés à la gestion et à la maintenance des portefeuilles, qui sont censés fonctionner conformément à la définition établie dans les politiques qui déterminent les processus. L'évaluation bisannuelle des vulnérabilités est une exigence découlant du règlement (UE) n° 910/2014, afin de garantir que la solution de portefeuille continue de couvrir de manière appropriée les risques et menaces liés à la cybersécurité identifiés dans le registre des risques, y compris toute évolution du panorama des menaces. Les notions d'évaluations de surveillance, d'évaluations de recertification et d'évaluations spéciales devraient être conformes à la norme EN ISO/IEC 17021-1:2015.

(25) Un cycle de certification prend fin avec l'expiration du certificat de conformité ou avec la délivrance d'un nouveau certificat de conformité faisant suite à une évaluation de recertification réussie. L'évaluation de recertification devrait comprendre une évaluation de tous les éléments de l'objet de la certification, y compris une évaluation de l'efficacité et, le cas échéant, une évaluation des vulnérabilités. Lors de la recertification, il devrait être possible de réutiliser les résultats des évaluations précédentes relatives à des éléments qui n'ont pas subi de modification.

(26) Lorsqu'un schéma européen de certification de cybersécurité est adopté, les schémas nationaux de certification ayant le même champ d'application devraient cesser de délivrer des certifications après une période de transition déterminée visée à l'article 57, paragraphe 1, du règlement (UE) 2019/881.

(27) Les schémas nationaux de certification devraient s'appuyer sur les cadres existants et réutiliser les éléments de preuve, le cas échéant, afin de garantir l'harmonisation et l'interopérabilité. Les États membres peuvent conclure des accords pour la réutilisation transfrontière de schémas de certification ou de parties de ces schémas. La Commission européenne et l'ENISA devraient, en coopération avec le groupe de coopération, aider les États membres à élaborer leurs schémas nationaux de certification et à en assurer la maintenance en veillant au partage des connaissances et au respect des bonnes pratiques.

(28) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([9]) et a rendu son avis le 30 septembre 2024.

(29) Les mesures prévues par le présent règlement sont conformes à l'avis du comité visé à l'article 48, paragraphe 1, du règlement (UE) n° 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet et champ d'application

Le présent règlement définit des normes de référence et établit des spécifications et des procédures visant à mettre en place un cadre solide pour la certification des portefeuilles, qui devra être régulièrement actualisé afin de rester en adéquation avec l'évolution des technologies et des normes et avec les travaux menés sur la base de la recommandation (UE) 2021/946 concernant une boîte à outils commune de l'Union pour une approche coordonnée en vue d'un cadre européen relatif à une identité numérique, et en particulier l'architecture et le cadre de référence.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

1) «solution de portefeuille»: une combinaison de logiciels, de matériel, de services, de paramètres et de configurations, y compris des instances de portefeuille, une ou plusieurs applications cryptographiques sécurisées de portefeuille et un ou plusieurs dispositifs cryptographiques sécurisés de portefeuille;

2) «propriétaire du schéma»: un organisme responsable de l'élaboration et de la maintenance d'un schéma de certification;

3) «objet de la certification»: les produits, processus et services, ou une combinaison de ceux-ci, auxquels s'appliquent des exigences précises;

4) «application cryptographique sécurisée de portefeuille»: une application qui gère des actifs critiques en étant liée aux fonctions cryptographiques et non cryptographiques fournies par le dispositif cryptographique sécurisé de portefeuille et en utilisant ces fonctions;

5) «instance de portefeuille»: l'application installée et configurée sur l'appareil ou dans l'environnement d'un utilisateur de portefeuille, qui fait partie d'une unité de portefeuille, et dont l'utilisateur du portefeuille se sert pour interagir avec l'unité de portefeuille;

([9]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

6) «dispositif cryptographique sécurisé de portefeuille»: un dispositif inviolable qui fournit un environnement lié à l'application cryptographique sécurisée de portefeuille et utilisé par celle-ci pour protéger les actifs critiques et fournir des fonctions cryptographiques pour l'exécution sécurisée d'opérations critiques;

7) «registre des risques»: un enregistrement des informations pertinentes pour le processus de certification concernant les risques identifiés;

8) «fournisseur de portefeuille»: une personne physique ou morale qui fournit des solutions de portefeuille;

9) «organisme de certification»: un organisme tiers d'évaluation de la conformité exploitant des schémas de certification;

10) «unité de portefeuille»: une configuration unique d'une solution de portefeuille comprenant des instances de portefeuille, des applications cryptographiques sécurisées de portefeuille et des dispositifs cryptographiques sécurisés de portefeuille, fournie par un fournisseur de portefeuille à un utilisateur de portefeuille donné;

11) «actifs critiques»: les actifs se trouvant à l'intérieur d'une unité de portefeuille ou en rapport avec celle-ci et dont l'importance est tellement exceptionnelle que la capacité de se fier à l'unité de portefeuille serait très sérieusement affaiblie si leur disponibilité, leur confidentialité ou leur intégrité étaient compromises;

12) «utilisateur de portefeuille»: un utilisateur qui contrôle l'unité de portefeuille;

13) «incident»: un incident au sens de l'article 6, point 6, de la directive (UE) 2022/2555 du Parlement européen et du Conseil ([10]);

14) «politique de divulgation intégrée»: un ensemble de règles, intégrées dans une attestation électronique d'attributs par le fournisseur de ces derniers, qui indique les conditions qu'une partie utilisatrice de portefeuille doit remplir pour accéder à l'attestation électronique d'attributs.

CHAPITRE II

SCHÉMAS NATIONAUX DE CERTIFICATION

Article 3

Mise en place de schémas nationaux de certification

1. Les États membres désignent un propriétaire du schéma pour chaque schéma national de certification.

2. L'objet de la certification défini dans les schémas nationaux de certification est la fourniture et l'exploitation de solutions de portefeuille et des schémas d'identification électronique dans le cadre duquel elles sont fournies.

3. Conformément au règlement d'exécution (UE) 2015/1502, l'objet de la certification dans les schémas nationaux de certification comprend les éléments suivants:

a) les composants logiciels, y compris les paramètres et les configurations d'une solution de portefeuille et du schéma d'identification électronique dans le cadre duquel les solutions de portefeuille sont fournies;

b) les composants matériels et les plateformes sur lesquels les composants logiciels visés au point b) fonctionnent ou dont ils dépendent pour des opérations d'importance critique, dans les cas où ils sont fournis directement ou indirectement par la solution de portefeuille et le schéma d'identification électronique dans le cadre desquels ils sont fournis et lorsqu'ils sont tenus d'atteindre le niveau de garantie souhaité pour ces composants logiciels. Lorsque les composants matériels et les plateformes ne sont pas fournis par le fournisseur de portefeuille, les schémas nationaux de certification formulent des hypothèses pour l'évaluation des composants matériels et des plateformes en vertu de laquelle une résistance peut être opposée aux attaquants à potentiel d'attaque élevé conformément au règlement d'exécution (UE) 2015/1502, et précisent les activités d'évaluation visant à confirmer ces hypothèses, visées à l'annexe IV;

([10]) 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, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

c) les processus qui soutiennent la fourniture et le fonctionnement d'une solution de portefeuille, y compris le processus d'enrôlement des utilisateurs visé à l'article 5 *bis* du règlement (UE) n° 910/2014, couvrant au moins l'inscription, la gestion des moyens électroniques et l'organisation conformément aux sections 2.1, 2.2 et 2.4 de l'annexe I du règlement d'exécution (UE) 2015/1502.

4. Les schémas nationaux de certification comprennent une description de l'architecture spécifique des solutions de portefeuille et du schéma d'identification électronique dans le cadre duquel elles sont fournies. Lorsque les schémas nationaux de certification couvrent plus d'une architecture spécifique, ils incluent un profil pour chacune de ces architectures.

5. Pour chaque profil, les schémas nationaux de certification définissent au moins les éléments suivants:

a) l'architecture spécifique d'une solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie;

b) les contrôles de sécurité associés aux niveaux de garantie énoncés à l'article 8 du règlement (UE) n° 910/2014;

c) un plan d'évaluation établi conformément au point 7.4.1 de la norme EN ISO/IEC 17065:2012;

d) les exigences de sécurité nécessaires pour faire face aux risques et menaces de cybersécurité énumérés dans le registre des risques figurant à l'annexe I du présent règlement, jusqu'au niveau de garantie requis, et pour atteindre, le cas échéant, les objectifs définis à l'article 51 du règlement (UE) 2019/881;

e) une mise en correspondance des contrôles visés au point b) du présent paragraphe avec les composantes de l'architecture;

f) une description de la manière dont les contrôles de sécurité, la mise en correspondance, les exigences de sécurité et le plan d'évaluation visés aux points b) à c) permettent aux fournisseurs de solutions de portefeuille et au schéma d'identification électronique dans le cadre duquel elles sont fournies de faire face de manière adéquate aux risques et menaces de cybersécurité identifiés dans le registre des risques visé au point d), jusqu'au niveau de garantie requis, en s'appuyant sur une analyse de risque permettant d'affiner et de compléter le registre des risques avec des risques et des menaces propres à l'architecture.

6. Le plan d'évaluation visé au paragraphe 5, point c), énumère les activités d'évaluation à inclure dans l'évaluation des solutions de portefeuille et du schéma d'identification électronique dans le cadre duquel elles sont fournies.

7. L'activité d'évaluation visée au paragraphe 6 exige des fournisseurs de solutions de portefeuille et du schéma d'identification électronique dans le cadre duquel ces solutions sont fournies qu'ils communiquent des informations répondant aux exigences énumérées à l'annexe II.

Article 4

Exigences d'ordre général

1. Les schémas nationaux de certification couvrent les exigences fonctionnelles, de cybersécurité et de protection des données en utilisant les schémas de certification suivants, lorsqu'ils sont disponibles et applicables:

a) les schémas européens de certification de cybersécurité établis en vertu du règlement (UE) 2019/881, notamment le schéma européen de certification de cybersécurité fondé sur des critères communs (EUCC);

b) les schémas nationaux de certification de cybersécurité couverts par l'EUCC, conformément à l'article 49 du règlement d'exécution (UE) 2024/482.

2. Les schémas nationaux de certification peuvent en outre faire référence, lorsqu'ils sont disponibles et applicables:

a) à d'autres schémas nationaux de certification pertinents;

b) à des normes internationales, européennes et nationales;

c) à des spécifications techniques qui satisfont aux exigences énoncées à l'annexe II du règlement (UE) nº 1025/2012 du Parlement européen et du Conseil ([11]).

3. Les schémas nationaux de certification:

a) précisent les éléments énumérés au point 6.5 de la norme EN ISO/IEC 17067:2013;

b) sont mis en œuvre sous la forme d'un schéma de type 6, conformément au point 5.3.8 de la norme EN ISO/IEC 17067:2013.

4. Les schémas nationaux de certification satisfont aux exigences suivantes:

a) seuls les fournisseurs visés à l'article 5 *bis*, paragraphe 2, du règlement (UE) nº 910/2014 peuvent se voir délivrer des certificats dans le cadre des schémas nationaux de certification;

b) seul le label de confiance est utilisé comme marque de conformité;

c) les fournisseurs de solutions de portefeuille et le schéma d'identification électronique dans le cadre duquel ces solutions sont fournies mentionnent des références au règlement (UE) nº 910/2014 et au présent règlement lorsqu'ils font référence au schéma;

d) les fournisseurs de solutions de portefeuille et le schéma d'identification électronique dans le cadre duquel ces solutions sont fournies complètent l'évaluation des risques du schéma visée à l'article 3, paragraphe 5, point f), afin de recenser les risques et les menaces propres à leur mise en œuvre de la solution et de proposer des mesures de traitement appropriées pour tous les risques et menaces pertinents;

e) les responsabilités et les recours juridictionnels sont établis et comprennent des références à la législation nationale applicable, qui définit les responsabilités et les voies de recours en cas d'utilisation frauduleuse de la certification relevant du schéma.

5. L'évaluation visée au paragraphe 4, point d), est communiquée à l'organisme de certification pour évaluation.

Article 5

Gestion des incidents et des vulnérabilités

1. Les schémas nationaux de certification contiennent des exigences en matière de gestion des incidents et des vulnérabilités conformément aux paragraphes 2 à 9.

2. Le titulaire du certificat de conformité d'une solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie notifie sans retard injustifié à son organisme de certification toute violation ou altération de la solution de portefeuille, ou du schéma d'identification électronique dans le cadre duquel elle est fournie, susceptible d'avoir une incidence sur sa conformité aux exigences des schémas nationaux de certification.

3. Le titulaire d'un certificat de conformité établit, tient à jour et applique une politique et des procédures en matière de gestion des vulnérabilités, compte tenu des procédures établies dans les normes internationales et européennes existantes, notamment EN ISO/IEC 30111:2019.

4. Le titulaire du certificat de conformité notifie à l'organisme de certification émetteur les vulnérabilités et les modifications affectant la solution de portefeuille, sur la base de critères définis concernant l'incidence de ces vulnérabilités et modifications.

5. Le titulaire du certificat de conformité établit un rapport d'analyse d'impact des vulnérabilités pour toute vulnérabilité affectant les composants logiciels de la solution de portefeuille. Le rapport comporte les informations suivantes:

a) l'impact de la vulnérabilité sur la solution de portefeuille certifiée;

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

([11]) Règlement (UE) nº 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision nº 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

c) les éventuelles possibilités de remédier à la vulnérabilité à l'aide des moyens disponibles;

d) lorsqu'il est possible de remédier à la vulnérabilité à l'aide des moyens disponibles, les manières envisageables pour y remédier.

6. Lorsqu'une notification est requise au paragraphe 4, le titulaire du certificat de conformité transmet sans retard injustifié à l'organisme de certification le rapport d'analyse d'impact des vulnérabilités mentionné au paragraphe 5.

7. Le titulaire d'un certificat de conformité établit, tient à jour et applique une politique de gestion des vulnérabilités satisfaisant aux exigences énoncées à l'annexe I du règlement sur la cyberrésilience ([12]).

8. Les schémas nationaux de certification établissent les exigences en matière de divulgation des vulnérabilités applicables aux organismes de certification.

9. Le titulaire d'un certificat de conformité divulgue et enregistre toute vulnérabilité connue du public et corrigée dans la solution de portefeuille ou dans l'un des répertoires en ligne visés à l'annexe V.

Article 6

Maintenance des schémas nationaux de certification

1. Les schémas nationaux de certification prévoient un processus de réexamen périodique de leur fonctionnement. Ce processus vise à confirmer leur caractère adéquat et à recenser les aspects à améliorer, en tenant compte des retours d'information des parties prenantes.

2. Les schémas nationaux de certification prévoient des dispositions relatives à leur maintenance. Ces dispositions comprennent au moins les exigences suivantes:

a) des règles concernant la gouvernance de la définition et des exigences des schémas nationaux de certification;

b) l'établissement de calendriers pour la délivrance des certificats à la suite de l'adoption de versions actualisées des schémas nationaux de certification, tant pour les nouveaux certificats de conformité que pour les certificats précédemment délivrés;

c) un réexamen périodique des schémas nationaux de certification, afin de veiller à l'application cohérente de leurs exigences, en tenant compte au moins des aspects suivants:

— les demandes de clarification adressées au propriétaire du schéma national de certification en ce qui concerne les exigences de ce schéma,

— le retour d'information des parties prenantes et des autres parties intéressées,

— la réactivité du propriétaire du schéma national de certification aux demandes d'informations;

d) les règles relatives au suivi des documents de référence et des procédures pour l'évolution des versions de référence des schémas nationaux de certification, y compris au moins les périodes de transition;

e) un processus visant à garantir que les risques et menaces les plus récents en matière de cybersécurité énumérés dans le registre des risques figurant à l'annexe I du présent règlement sont couverts;

f) un processus relatif à la gestion d'autres modifications dans les schémas nationaux de certification.

([12]) 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) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience) (JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

3. Les schémas nationaux de certification contiennent des exigences relatives à la réalisation d'évaluations des produits actuellement certifiés dans un certain délai après la révision du schéma, ou après la publication de nouvelles spécifications ou normes, ou de nouvelles versions de celles-ci, auxquelles les solutions de portefeuille et le schéma d'identification électronique dans le cadre duquel elles sont fournies doivent être conformes.

CHAPITRE III

EXIGENCES RELATIVES AUX PROPRIÉTAIRES DE SCHÉMAS

Article 7

Exigences d'ordre général

1. Les propriétaires de schémas élaborent et maintiennent des schémas nationaux de certification et régissent leurs activités.

2. Les propriétaires de schémas peuvent sous-traiter tout ou partie de leurs tâches à un tiers. Lorsqu'ils sous-traitent à une partie privée, les propriétaires de schémas définissent par contrat les obligations et les responsabilités de toutes les parties. Les propriétaires de schémas restent responsables de toutes les activités sous-traitées réalisées par leurs sous-traitants.

3. Les propriétaires de schémas exercent leurs activités de surveillance, le cas échéant, au moins sur la base des informations suivantes:

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

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

c) réclamations et recours introduits en application de l'article 15.

4. Les propriétaires de schémas informent le groupe de coopération des révisions des schémas nationaux de certification. Cette notification fournit au groupe de coopération des informations adéquates lui permettant de formuler des recommandations à l'intention des propriétaires de schémas et des avis sur les schémas nationaux de certification mis à jour.

CHAPITRE IV

EXIGENCES RELATIVES AUX FOURNISSEURS DE SOLUTIONS DE PORTEFEUILLE ET AU SCHÉMA D'IDENTIFICATION ÉLECTRONIQUE DANS LE CADRE DUQUEL CES SOLUTIONS SONT FOURNIES

Article 8

Exigences d'ordre général

1. Les schémas nationaux de certification contiennent des exigences en matière de cybersécurité fondées sur une évaluation des risques pour chaque architecture prise en charge. Ces exigences en matière de cybersécurité visent à traiter les risques et menaces de cybersécurité identifiés, tels qu'énumérés dans le registre des risques figurant à l'annexe I.

2. Conformément à l'article 5 *bis*, paragraphe 23, du règlement (UE) n° 910/2014, les schémas nationaux de certification exigent que les solutions de portefeuille et les schémas d'identification électronique dans le cadre desquels elles sont fournies résistent à des attaquants à potentiel d'attaque élevé et présentent donc un niveau de garantie élevé, conformément au règlement d'exécution (UE) 2015/1502.

3. Les schémas nationaux de certification établissent des critères de sécurité qui comprennent les exigences suivantes:

a) celles du règlement sur la cyberrésilience, le cas échéant, ou les exigences répondant aux objectifs de sécurité énoncés à l'article 51 du règlement (UE) 2019/881;

b) l'établissement et la mise en œuvre de politiques et de procédures concernant la gestion des risques liés à l'exploitation d'une solution de portefeuille, y compris l'identification et l'évaluation des risques et l'atténuation des risques identifiés;

c) l'établissement et la mise en œuvre de politiques et de procédures relatives à la gestion des modifications et à la gestion des vulnérabilités conformément à l'article 5 du présent règlement;

d) l'établissement et la mise en œuvre de politiques et de procédures de gestion des ressources humaines, y compris des exigences en matière d'expertise, de fiabilité, d'expérience, de formation en matière de sécurité et de qualifications du personnel participant au développement ou à l'exploitation de la solution de portefeuille;

e) les exigences relatives à l'environnement d'exploitation de la solution de portefeuille, notamment sous la forme d'hypothèses concernant la sécurité des dispositifs et plateformes sur lesquels fonctionnent les composants logiciels de la solution de portefeuille, y compris les WSCD et, si nécessaire et le cas échéant, les exigences en matière d'évaluation de la conformité permettant de confirmer que ces hypothèses sont vérifiées sur les dispositifs et plateformes concernés;

f) pour toute hypothèse qui n'est pas étayée par un certificat de conformité ou d'autres informations acceptables en matière de garantie, une description du mécanisme que le fournisseur de portefeuille utilise pour étayer l'hypothèse, ainsi qu'une justification du fait que le mécanisme est suffisant pour faire en sorte que l'hypothèse soit vérifiée;

g) la mise en place et l'application de mesures qui garantissent que la version de la solution de portefeuille actuellement utilisée est certifiée.

4. Les schémas nationaux de certification contiennent des exigences fonctionnelles relatives aux mécanismes de mise à jour pour chaque composant logiciel des solutions de portefeuille et du schéma d'identification électronique dans le cadre duquel ces solutions sont fournies pour les opérations énumérées à l'annexe III.

5. Les schémas nationaux de certification exigent que les informations et documents suivants soient fournis ou mis à la disposition de l'organisme de certification par le demandeur de la certification:

a) les éléments de preuve relatifs aux informations visées à l'annexe IV, point 1, y compris, le cas échéant, des précisions sur la solution de portefeuille et son code source, telles que:

— *des informations sur l'architecture*: pour chaque composant de la solution de portefeuille (y compris les composants de produits, de processus et de services), une description de ses propriétés essentielles de sécurité, notamment ses dépendances externes,

— *des contrôles et des niveaux de garantie*: pour chaque contrôle de sécurité de la solution de portefeuille, une description du contrôle et du niveau de garantie requis, sur la base de l'annexe du règlement d'exécution (UE) 2015/1502, qui définit un certain nombre de spécifications techniques et de procédures applicables aux différents contrôles mis en œuvre par les moyens d'identification électronique,

— *une mise en correspondance des contrôles avec les composantes de l'architecture*: une description de la manière dont les contrôles du portefeuille sont mis en œuvre à l'aide des différents composants de la solution de portefeuille, fondée sur un exposé des motifs pour lesquels un certain niveau de garantie est requis, et une explication de la manière dont le contrôle est mis en œuvre avec tous les aspects de sécurité requis au niveau approprié,

— *une motivation et une justification de la couverture des risques*: une justification:

— de la mise en correspondance des contrôles avec les composants,

— de la pertinence du plan d'évaluation proposé pour que tous les contrôles soient couverts de manière appropriée,

— la couverture fournie par les contrôles des risques et menaces liés à la cybersécurité recensés dans le registre des risques, complétés par des contrôles des risques et des menaces spécifiques à la mise en œuvre, au niveau de garantie approprié;

b) les informations énumérées à l'annexe V;

c) une liste complète des certificats de conformité et des autres informations en matière de garantie utilisées comme preuves au cours des activités d'évaluation;

d) toute autre information pertinente pour les activités d'évaluation.

CHAPITRE V

EXIGENCES RELATIVES AUX ORGANISMES DE CERTIFICATION

Article 9

Exigences d'ordre général

1. Les organismes de certification sont accrédités par des organismes nationaux d'accréditation désignés en application du règlement (CE) nº 765/2008 du Parlement européen et du Conseil ([13]) conformément à la norme EN ISO/IEC 17065:2012, pour autant qu'ils satisfassent aux exigences énoncées dans les schémas nationaux de certification conformément au paragraphe 2.

2. Aux fins de l'accréditation, les organismes de certification satisfont à toutes les exigences de compétence suivantes:

a) connaissance détaillée et technique des architectures pertinentes d'une solution de portefeuille et du schéma d'identification électronique dans le cadre duquel celle-ci est fournie, ainsi que des menaces et des risques pertinents pour ces architectures;

b) connaissance des solutions de sécurité disponibles et de leurs propriétés conformément à l'annexe du règlement d'exécution (UE) 2015/1502;

c) connaissance des activités exécutées au titre des certificats de conformité appliqués aux composants de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel celle-ci est fournie, comme faisant l'objet de la certification;

d) connaissance détaillée du schéma national de certification applicable établi conformément au chapitre II.

3. Les organismes de certification exercent leurs activités de surveillance notamment sur la base des informations suivantes:

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

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

c) réclamations et recours introduits en application de l'article 15.

Article 10

Sous-traitance

Les organismes de certification peuvent sous-traiter les activités d'évaluation visées à l'article 13 à des tiers. Lorsque les activités d'évaluation sont sous-traitées, les schémas nationaux de certification établissent:

1) que tous les sous-traitants de l'organisme de certification effectuant des activités d'évaluation satisfont, le cas échéant et en fonction des activités à réaliser, aux exigences de normes harmonisées telles que EN ISO/IEC 17025:2017 pour les essais, EN ISO/IEC 17020:2012 pour l'inspection, EN ISO/IEC 17021-1:2015 pour l'audit et EN ISO/IEC 17029:2019 pour la validation et la vérification;

2) que les organismes de certification assument la responsabilité de toutes les activités d'évaluation sous-traitées à d'autres organismes et démontrent qu'ils ont pris les mesures appropriées au cours de leur accréditation, y compris en s'appuyant, le cas échéant, sur leur propre accréditation de leurs sous-traitants;

3) dans quelle mesure un accord préalable à la sous-traitance doit être obtenu auprès des propriétaires de schémas ou du client dont la solution de portefeuille est certifiée dans le cadre du schéma de certification.

([13]) Règlement (CE) nº 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) nº 339/93 (JO L 218 du 13.8.2008, p. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

Article 11

Notification à l'organe de contrôle

Les organismes de certification notifient à l'organe de contrôle visé à l'article 46 *bis*, paragraphe 1, du règlement (UE) n° 910/2014 la délivrance, la suspension et l'annulation des certificats de conformité d'une solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie.

Article 12

Gestion des incidents et des vulnérabilités

1. Les organismes de certification suspendent, sans retard injustifié, le certificat de conformité des solutions de portefeuille et du schéma d'identification électronique dans le cadre duquel elles sont fournies après avoir confirmé que l'atteinte à la sécurité ou l'altération notifiée a un impact sur la conformité avec les exigences des schémas nationaux de certification de la solution de portefeuille ou du schéma d'identification électronique dans le cadre duquel elle est fournie.

2. Les organismes de certification annulent le certificat de conformité qui a été suspendu à la suite d'une atteinte à la sécurité ou d'une altération à laquelle il n'a pas été remédié en temps utile.

3. Les organismes de certification annulent les certificats de conformité lorsqu'il n'a pas été remédié en temps utile à une vulnérabilité identifiée de manière proportionnée à sa gravité et à son impact potentiel, conformément à l'article 5 *quater*, paragraphe 4, et à l'article 5 *sexies*, paragraphe 2, du règlement (UE) n° 910/2014.

CHAPITRE VI

ACTIVITÉS D'ÉVALUATION DE LA CONFORMITÉ

Article 13

Activités d'évaluation

1. Les schémas nationaux de certification contiennent les méthodes et procédures à utiliser par les organismes d'évaluation de la conformité dans le cadre de leurs activités d'évaluation conformément à la norme EN ISO/IEC 17065:2012, qui couvrent au moins les aspects suivants:

a) les méthodes et procédures permettant d'exécuter les activités d'évaluation, y compris celles liées au WSCD, comme indiqué à l'annexe IV;

b) l'audit de la mise en œuvre de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie, sur la base du registre des risques figurant à l'annexe I complété, si nécessaire, par des risques propres à la mise en œuvre;

c) les activités de test fonctionnel, fondées, lorsqu'elles sont disponibles et appropriées, sur des suites d'essais définies conformément aux spécifications ou normes techniques;

d) l'évaluation de l'existence et de l'adéquation des processus de maintenance, y compris au moins la gestion de la version, la gestion des mises à jour et la gestion des vulnérabilités;

e) l'évaluation de l'efficacité opérationnelle des processus de maintenance, y compris au moins la gestion de la version, la gestion des mises à jour et la gestion des vulnérabilités;

f) l'analyse des dépendances communiquée par le fournisseur de portefeuille, notamment une méthode d'évaluation de l'acceptabilité des informations en matière de garantie, qui comprend les éléments énoncés à l'annexe VI;

g) l'évaluation des vulnérabilités, au niveau approprié, y compris:

— un examen de la conception de la solution de portefeuille et, le cas échéant, de son code source,

— des tests de résistance de la solution de portefeuille à des attaquants à potentiel d'attaque élevé pour le niveau de garantie «élevé» conformément à la section 2.2.1 de l'annexe du règlement d'exécution (UE) 2015/1502;

h) l'évaluation de l'évolution de l'environnement de menaces et de son impact sur la couverture des risques par la solution de portefeuille, afin de déterminer les activités d'évaluation à exécuter sur les différents composants de la solution de portefeuille.

2. Les schémas nationaux de certification contiennent une évaluation visant à déterminer si la mise en œuvre de solutions de portefeuille et le schéma d'identification électronique dans le cadre duquel ces solutions sont fournies correspondent à l'architecture définie à l'article 3, paragraphe 5, point a), ainsi qu'une évaluation visant à déterminer si le plan d'évaluation proposé conjointement avec la mise en œuvre correspond au plan d'évaluation visé à l'article 3, paragraphe 5, point c).

3. Les schémas nationaux de certification définissent des règles d'échantillonnage de manière à éviter de reproduire des activités d'évaluation identiques et afin de se concentrer sur des activités spécifiques à une variante donnée. Ces règles d'échantillonnage permettent de ne réaliser des tests fonctionnels et des tests de sécurité que sur un échantillon de variantes d'un composant cible de solution de portefeuille et du schéma d'identification électronique dans le cadre duquel la solution est fournie et sur un échantillon de dispositifs cibles. Les schémas nationaux de certification exigent de tous les organismes de certification qu'ils justifient leur recours à l'échantillonnage.

4. Les schémas nationaux de certification exigent que l'organisme de certification évalue la WSCA sur la base des méthodes et procédures décrites à l'annexe IV.

Article 14

Activités de certification

1. Les schémas nationaux de certification prévoient une activité d'attestation pour la délivrance d'un certificat de conformité, conformément à la norme EN ISO/IEC 17067:2013, tableau 1, section V a), portant notamment sur:

a) le contenu du certificat de conformité prévu à l'annexe VII;

b) la manière dont les résultats de l'évaluation doivent être consignés dans le rapport public de certification, y compris au moins un résumé du plan préliminaire d'audit et de validation, comme indiqué à l'annexe VIII;

c) le contenu des résultats de l'évaluation consignés dans le rapport d'évaluation de la certification, y compris les éléments énoncés à l'annexe VIII.

2. Le rapport d'évaluation de la certification peut être mis à la disposition du groupe de coopération et de la Commission.

Article 15

Réclamations et recours

Les schémas nationaux de certification contiennent des procédures ou des références à la législation nationale applicable, qui définissent le mécanisme relatif à l'introduction et au traitement efficaces de réclamations et de recours liés à leur mise en œuvre du schéma de certification ou à un certificat de conformité délivré. Ces procédures comprennent la communication à l'auteur de la réclamation d'informations sur l'état d'avancement de la procédure et sur la décision prise ainsi que sur le droit à un recours juridictionnel effectif. Les schémas nationaux de certification exigent que toutes les réclamations et tous les recours qui n'ont pas été résolus ou qui ne peuvent pas être résolus par l'organisme de certification soient envoyés au propriétaire du schéma pour évaluation et résolution.

Article 16

Activités de surveillance

1. Les schémas nationaux de certification exigent que les organismes de certification mettent en œuvre des activités de surveillance consistant en une évaluation de processus combinée à des tests ou inspections aléatoires.

2. Les schémas nationaux de certification contiennent des exigences imposant aux propriétaires de schémas de contrôler le respect, par les organismes de certification, des obligations qui leur incombent en vertu du règlement (UE) n° 910/2014 et des schémas nationaux de certification, le cas échéant.

3. Les schémas nationaux de certification contiennent des exigences imposant aux organismes de certification de contrôler les éléments suivants:

a) le respect, par les titulaires d'un certificat de conformité délivré dans le cadre de schémas nationaux de certification, des obligations qui leur incombent en matière de certification en vertu du règlement (UE) nº 910/2014 et des schémas nationaux de certification;

b) la conformité de la solution de portefeuille certifiée aux exigences énoncées dans les schémas nationaux de certification.

Article 17

Conséquences en cas de non-respect

Les schémas nationaux de certification définissent les conséquences de la non-conformité d'une solution de portefeuille certifiée et du schéma d'identification électronique dans le cadre duquel elle est fournie avec les exigences énoncées dans le présent règlement. Ces conséquences comprennent notamment:

1) l'obligation faite à l'organisme de certification d'informer le titulaire du certificat de conformité et de lui demander d'appliquer des mesures correctives;

2) l'obligation faite à l'organisme de certification d'informer les autres autorités de surveillance du marché concernées lorsque la non-conformité concerne la législation pertinente de l'Union;

3) les conditions d'exécution des actions correctives par le titulaire du certificat de conformité;

4) les conditions de suspension d'un certificat de conformité par l'organisme de certification et de rétablissement du certificat de conformité après qu'il a été remédié à la non-conformité;

5) les conditions d'annulation d'un certificat de conformité par l'organisme de certification;

6) les conséquences du non-respect, par l'organisme de certification, des exigences du schéma national de certification.

CHAPITRE VII

CYCLE DE VIE DE LA CERTIFICATION

Article 18

Cycle de vie de la certification

1. La validité des certificats de conformité délivrés dans le cadre de schémas nationaux de certification fait l'objet d'activités d'évaluation régulières exécutées par l'organisme de certification conformément aux exigences énoncées à l'annexe IX.

2. Les schémas nationaux de certification contiennent un processus de recertification des solutions de portefeuille et du schéma d'identification électronique dans le cadre duquel elles sont fournies, à la demande du titulaire du certificat de conformité avant l'expiration du certificat de conformité initial. Ce processus de recertification comprend une évaluation complète de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie, y compris une évaluation des vulnérabilités, conformément aux principes énoncés à l'annexe IX.

3. Les schémas nationaux de certification contiennent une procédure pour la gestion des modifications apportées à une solution de portefeuille certifiée et au schéma d'identification électronique dans le cadre duquel elle est fournie. Cette procédure comprend des règles permettant de déterminer si une modification doit être soumise à l'évaluation spéciale mentionnée au paragraphe 4 ou à la vérification de l'efficacité opérationnelle des processus de maintenance mentionnée à l'annexe IV.

4. Les schémas nationaux de certification contiennent une procédure relative aux évaluations spéciales conforme à la norme EN ISO/IEC 17065:2012. Cette procédure comprend une série d'activités à réaliser pour résoudre le problème spécifique qui a rendu nécessaire l'évaluation spéciale.

5. Les schémas nationaux de certification établissent les règles applicables à l'annulation d'un certificat de conformité.

CHAPITRE VIII

ENREGISTREMENTS ET PROTECTION DES INFORMATIONS

Article 19

Conservation des enregistrements

1. Les schémas nationaux de certification contiennent des dispositions applicables aux organismes de certification concernant un système permettant d'enregistrer toutes les informations pertinentes produites en lien avec les activités d'évaluation de la conformité qu'ils réalisent, y compris les données délivrées et reçues par les fournisseurs de solutions de portefeuille et les schémas d'identification électronique dans le cadre desquels ces solutions sont fournies. Les enregistrements de ces informations sont conservés de manière sécurisée. Les enregistrements peuvent être conservés sous forme électronique et restent accessibles aussi longtemps que le droit de l'Union ou le droit national l'exige, et pendant au moins cinq ans après l'annulation ou l'expiration du certificat de conformité correspondant.

2. Les schémas nationaux de certification imposent au titulaire du certificat de conformité de conserver de manière sécurisée les informations suivantes aux fins du présent règlement, et ce pendant au moins cinq ans après l'annulation ou l'expiration du certificat de conformité correspondant:

a) les enregistrements des informations fournies à l'organisme de certification ou à l'un quelconque de ses sous-traitants au cours de la procédure de certification;

b) des échantillons de composants matériels qui relèvent du champ d'application de la certification de la solution de portefeuille.

3. Les schémas nationaux de certification exigent du titulaire du certificat de conformité qu'il mette, sur demande, les informations visées au paragraphe 1 à la disposition de l'organisme de certification ou de l'organe de contrôle visé à l'article 46 *bis*, paragraphe 1, du règlement (UE) n° 910/2014.

Article 20

Protection des informations

Dans le cadre des schémas nationaux de certification, toutes les personnes ou organisations qui se voient accorder l'accès à des informations au titre de l'exécution d'activités relevant du schéma national de certification sont tenues d'assurer la sécurité et la protection des secrets d'affaires et autres informations confidentielles, ainsi que de préserver les droits de propriété intellectuelle, et de prendre les mesures techniques et organisationnelles nécessaires et appropriées pour garantir cette confidentialité.

CHAPITRE IX

DISPOSITIONS FINALES

Article 21

Transition vers un schéma européen de certification de cybersécurité

Le présent règlement fait l'objet d'un réexamen, lors de l'adoption du premier schéma européen de certification de cybersécurité pour les solutions de portefeuille et les schémas d'identification électronique dans le cadre desquels celles-ci sont fournies, dans le but de tenir compte de la contribution de ce schéma à la certification globale des solutions de portefeuille et des schémas d'identification électronique dans le cadre desquels elles sont fournies.

Article 22

Entrée en vigueur

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 2024.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE I

REGISTRE DES RISQUES POUR LES PORTEFEUILLES EUROPÉENS D'IDENTITÉ NUMÉRIQUE

Introduction

Le registre des risques décrit les principaux risques et menaces pour la sécurité et la vie privée qui s'appliquent aux portefeuilles et qui doivent être dûment pris en compte dans toute architecture et mise en œuvre des portefeuilles. Les **risques de haut niveau** (section I) sont liés à l'utilisation des portefeuilles par les utilisateurs et les parties utilisatrices et sont associés à des menaces directes ciblant les actifs des portefeuilles. En outre, quelques **risques systémiques** (section II) ont été identifiés pour les portefeuilles, qui résulteraient généralement d'une combinaison de menaces s'appliquant à l'ensemble du système de portefeuille.

Type de risque	Identifiant du risque	Intitulés des risques correspondants
Risques de haut niveau pour les portefeuilles	R1	Création ou utilisation d'une identité électronique existante
	R2	Création ou utilisation d'une fausse identité électronique
	R3	Création ou utilisation de faux attributs
	R4	Vol d'identité
	R5	Vol de données
	R6	Divulgation de données
	R7	Manipulation de données
	R8	Perte de données
	R9	Transaction non autorisée
	R10	Manipulation de transactions
	R11	Répudiation
	R12	Divulgation de données relatives aux transactions
	R13	Interruption de service
	R14	Surveillance
Risques systémiques	SR1	Surveillance de masse
	SR2	Préjudice de réputation
	SR3	Non-respect de la législation

Le registre recense également les **menaces techniques** (section III) qui ciblent la mise en œuvre de la solution de portefeuille. Ces menaces sont liées aux risques de haut niveau en ce sens que chacune d'entre elles pourrait être utilisée pour déclencher de nombreux risques de haut niveau.

Type de menace	Identifiant de la menace	Intitulés des menaces correspondantes	Sous-catégories de menaces
Menace technique	TT1	Attaques physiques	1.1. *Vol*
			1.2. *Fuite d'informations*
			1.3. *Manipulation frauduleuse*
	TT2	Erreurs et mauvaises configurations	2.1. *Erreurs commises dans la gestion d'un système informatique*
			2.2. *Erreurs au niveau de l'application ou erreurs d'utilisation*
			2.3. *Erreurs dans la phase de développement et mauvaises configurations des systèmes*

Type de menace	Identifiant de la menace	Intitulés des menaces correspondantes	Sous-catégories de menaces
	TT3	Utilisation de ressources non fiables	3.1. *Utilisation ou configuration erronées des composants du portefeuille*
	TT4	Défaillance et pannes	4.1. *Défaillance ou dysfonctionnement des équipements, appareils ou systèmes*
			4.2. *Perte de ressources*
			4.3. *Perte de services d'appui*
	TT5	Actions malveillantes	5.1. *Interception d'informations*
			5.2. *Hameçonnage et usurpation*
			5.3. *Rejeu de messages*
			5.4. *Attaque par force brute*
			5.5. *Vulnérabilités logicielles*
			5.6. *Attaques contre la chaîne logistique*
			5.7. *Maliciels*
			5.8. *Prédiction de nombres aléatoires*

Enfin, le registre **énumère les menaces directes pour les portefeuilles**, chacune étant associée à une sélection (non exhaustive) de risques (section IV).

SECTION I

Risques de haut niveau pour les portefeuilles

R1. Création ou utilisation d'une identité électronique existante

La création ou l'utilisation d'une identité électronique existante est définie comme la création d'une identité électronique dans un portefeuille qui existe dans le monde réel et qui est attribuée à un autre utilisateur. Par nature, ce risque donne lieu à des risques de vol d'identité (R4) et de transactions non autorisées (R9).

R2. Création ou utilisation d'une fausse identité électronique

La création ou l'utilisation d'une fausse identité électronique est définie comme la création d'une identité électronique dans un portefeuille qui n'existe pas dans le monde réel.

R3. Création ou utilisation de faux attributs

La création ou l'utilisation de faux attributs est définie comme la création ou l'utilisation d'attributs dont la délivrance par le fournisseur déclaré ne peut pas être validée et qui ne sont pas fiables.

R4. Vol d'identité

Le vol d'identité est défini comme l'acquisition non autorisée de l'unité de portefeuille ou la perte de facteurs d'authentification permettant d'usurper l'identité d'une personne.

R5. Vol de données

Le vol de données est défini comme l'extraction non autorisée de données. Le vol de données est également associé à des menaces, telles que l'interception de données (captage non autorisé de données en transit) et le décryptage de données (décodage non autorisé de données cryptées), qui sont susceptibles d'entraîner, dans certains cas, la divulgation de données (R6).

R6. Divulgation de données

La divulgation de données est définie comme la divulgation non autorisée de données à caractère personnel, y compris de catégories particulières de données à caractère personnel. Le risque de violation de la vie privée est très similaire si l'on se place du point de vue de la protection de la vie privée plutôt que de celui de la sécurité.

R7. Manipulation de données

La manipulation de données est définie comme la modification non autorisée de données.

R8. Perte de données

La perte de données est définie comme la situation dans laquelle les données stockées dans le portefeuille sont perdues à la suite d'une utilisation abusive ou d'une action malveillante. Ce risque est souvent un risque accessoire de la manipulation de données (R7) ou de l'interruption de service (R13), caractérisé par l'impossibilité de rétablir des données en totalité ou en partie.

R9. Transaction non autorisée

Les transactions non autorisées sont définies comme des activités opérationnelles menées sans l'autorisation ou à l'insu de l'utilisateur du portefeuille. Dans de nombreux cas, une transaction non autorisée peut entraîner le vol d'identité (R4) ou la divulgation de données (R6). Elle est également liée à des transactions non autorisées, telles que l'utilisation abusive de clés cryptographiques.

R10. Manipulation de transactions

La manipulation de transactions est définie comme la modification non autorisée d'opérations dans le portefeuille. La manipulation de transactions est une atteinte à l'intégrité et est liée à une violation de l'intégrité des données.

R11. Répudiation

La répudiation est définie comme une situation dans laquelle une partie prenante peut refuser d'exécuter une action ou d'être associée à une transaction sans que les autres parties prenantes ne disposent d'éléments suffisants pour la contredire.

R12. Divulgation de données relatives aux transactions

La divulgation de données relatives aux transactions est définie comme la divulgation d'informations relatives à une transaction entre parties prenantes.

R13. Interruption de service

L'interruption de service est définie comme une interruption ou une dégradation du fonctionnement normal du portefeuille. Un type particulier d'interruption de service réside dans le blocage d'utilisateur, qui se définit comme l'impossibilité pour un utilisateur d'accéder à son compte ou à son portefeuille.

R14. Surveillance

La surveillance, ou écoute, est définie comme la surveillance ou l'observation non autorisée des activités, des communications ou des données d'un utilisateur de portefeuille. La surveillance est souvent associée à l'inférence, qui est définie comme la déduction d'informations sensibles ou personnelles à partir de données a priori inoffensives.

SECTION II

Risques systémiques

Ces risques ne sont pas utilisés dans la liste des menaces, car ils sont généralement la conséquence de menaces multiples, répétées d'une manière qui menace l'ensemble du système.

SR1. Surveillance de masse

La surveillance de masse est définie comme la surveillance ou l'observation des activités de nombreux utilisateurs par l'intermédiaire des communications ou des données de leur portefeuille. La surveillance de masse est souvent associée à la surveillance (R14) et à l'inférence à l'échelle mondiale, des informations sur un grand nombre d'utilisateurs étant combinées pour en déduire des données sensibles ou à caractère personnel concernant les utilisateurs ou pour déterminer des tendances statistiques susceptibles d'être utilisées pour concevoir de nouvelles attaques.

SR2. Préjudice de réputation

Le préjudice de réputation est défini comme le préjudice causé à la réputation d'une organisation ou d'un organisme gouvernemental. Le préjudice de réputation découlera également d'autres risques lorsqu'une violation ou un incident est couvert par les médias et dépeint l'organisation sous un jour défavorable. Le préjudice de réputation peut entraîner d'autres risques, tels que la perte de confiance, découlant des doutes raisonnables de l'utilisateur, et la perte de l'écosystème, lorsque l'ensemble de l'écosystème s'effondre.

SR3. Non-respect de la législation

Le non-respect de la législation est défini comme une situation dans laquelle les lois, règlements ou normes applicables ne peuvent pas être respectés. Dans le cadre du portefeuille, étant donné que la sécurité et le respect de la vie privée de la solution sont des exigences légales, toutes les menaces sont susceptibles d'entraîner une forme de non-respect de la législation.

SECTION III

Menaces techniques

Les menaces techniques ne sont pas toutes liées à des risques spécifiques pesant sur les portefeuilles, car beaucoup d'entre elles sont des moyens qui pourraient être utilisés pour mettre en œuvre des attaques correspondant à de nombreux risques différents.

TT1. Attaques physiques

1.1. *Vol*

Le vol est défini comme le vol de dispositifs pouvant altérer le bon fonctionnement du portefeuille (en cas de vol et de protection insuffisante de l'unité de portefeuille). Il peut donner lieu à de nombreux risques, dont le vol d'identité (R4), le vol de données (R5) et les transactions non autorisées (R9).

1.2. *Fuite d'informations*

La fuite d'informations est définie comme l'accès, la divulgation d'informations ou le partage non autorisés après l'accès physique au portefeuille. Elle peut notamment donner lieu à la divulgation de données (R6) et au vol de données (R5).

1.3. *Manipulation frauduleuse*

La manipulation est définie comme une atteinte à l'intégrité d'un ou de plusieurs composants de l'unité de portefeuille ou des composants dont dépend l'unité de portefeuille, tels que l'appareil de l'utilisateur ou son système d'exploitation. Elle peut notamment donner lieu à la manipulation de données (R7), à la perte de données (R8) et à la manipulation de transactions (R10). Lorsque la manipulation cible des composants logiciels, elle peut donner lieu à de nombreux risques.

TT2. Erreurs et mauvaises configurations

2.1. *Erreurs commises dans la gestion d'un système informatique*

Les erreurs commises dans la gestion d'un système informatique sont définies comme des fuites d'informations, un partage d'informations ou des dommages causés par l'utilisation abusive de ressources informatiques par les utilisateurs (méconnaissance des éléments de l'application) ou par une configuration ou une gestion inadéquate des ressources informatiques.

2.2. *Erreurs au niveau de l'application ou erreurs d'utilisation*

Les erreurs au niveau de l'application ou les erreurs d'utilisation sont définies comme des dysfonctionnements de l'application dus à une erreur dans l'application elle-même ou à une erreur de l'un des utilisateurs (utilisateurs de portefeuille et parties utilisatrices de portefeuille).

2.3. *Erreurs dans la phase de développement et mauvaises configurations des systèmes*

Les erreurs dans la phase de développement et les mauvaises configurations des systèmes sont définies comme des dysfonctionnements ou des vulnérabilités dus à des ressources informatiques ou à des processus opérationnels mal développés ou configurés (spécifications inadéquates des produits informatiques, utilisabilité insuffisante, interfaces mal sécurisées, flux de procédures et politiques inappropriés, erreurs de conception).

TT3. Utilisation de ressources non fiables

L'utilisation de ressources non fiables est définie comme une activité conduisant à des dommages involontaires dus à des relations de confiance mal définies, comme la confiance accordée à un fournisseur tiers sans garantie suffisante.

3.1. *Utilisation ou configuration erronées des composants du portefeuille*

Une utilisation ou une configuration erronée des composants du portefeuille est définie comme une détérioration involontaire des composants du portefeuille en raison d'une utilisation erronée ou d'une mauvaise configuration par les utilisateurs du portefeuille ou par des développeurs insuffisamment formés, ou en raison d'un manque d'adaptation aux changements dans le panorama des menaces, consistant classiquement à utiliser des plateformes d'exécution ou des composants de tiers vulnérables.

TT4. Défaillance et pannes

4.1. *Défaillance ou dysfonctionnement des équipements, appareils ou systèmes*

Les défaillances ou les dysfonctionnements d'un équipement sont définis comme une détérioration involontaire de ressources informatiques due à une défaillance ou un dysfonctionnement de l'équipement, comprenant l'infrastructure du fournisseur et les appareils des utilisateurs.

4.2. *Perte de ressources*

La perte de ressources est définie comme une panne ou un dysfonctionnement imputable à l'indisponibilité de ces ressources, par exemple dans le cas de pièces d'entretien.

4.3. *Perte de services d'appui*

La perte de services d'appui est définie comme une panne ou un dysfonctionnement imputable à l'indisponibilité des services d'appui nécessaires au bon fonctionnement du système, comprenant la connectivité au réseau de l'infrastructure du fournisseur et de l'appareil de l'utilisateur.

TT5. Actions malveillantes

5.1. *Interception d'informations*

L'interception d'informations est définie comme le captage d'informations mal sécurisées lors de leur transmission, comprenant les attaques de l'homme du milieu.

5.2. *Hameçonnage et usurpation*

L'hameçonnage est défini comme le captage d'informations fournies par l'utilisateur à la suite d'une interaction trompeuse, souvent associé à l'usurpation de moyens de communication et de sites web légitimes. Ces menaces ciblent l'utilisateur et contribuent classiquement au vol d'identité (R4) et aux transactions non autorisées (R9), en passant souvent par le vol de données (R5) ou la divulgation de données (R6).

5.3. *Rejeu de messages*

Le rejeu de messages est défini comme la réutilisation de messages précédemment interceptés pour effectuer des transactions non autorisées, souvent au niveau du protocole. Cette menace technique donne lieu principalement à des transactions non autorisées, qui peuvent entraîner par la suite d'autres risques, en fonction de la transaction.

5.4. *Attaque par force brute*

L'attaque par force brute est définie comme une atteinte à la sécurité, souvent à la confidentialité, par la réalisation d'un grand nombre d'interactions jusqu'à ce que les réponses fournissent des informations précieuses.

5.5. *Vulnérabilités logicielles*

La menace liée aux vulnérabilités logicielles est une atteinte à la sécurité par l'exploitation d'une vulnérabilité logicielle dans les composants du portefeuille ou dans les composants logiciels et matériels utilisés dans la mise en œuvre du portefeuille, comprenant les vulnérabilités publiées et les vulnérabilités non publiées (jour zéro).

5.6. *Attaques contre la chaîne logistique*

Une attaque contre la chaîne logistique est définie comme une atteinte à la sécurité par des attaques perpétrées contre le fournisseur de portefeuille ou ses utilisateurs afin de permettre d'autres attaques contre le portefeuille lui-même.

5.7. *Maliciels*

Les maliciels sont définis comme une atteinte à la sécurité par des applications malveillantes effectuant des actions non désirées et illégitimes sur le portefeuille.

5.8. *Prédiction de nombres aléatoires*

La prédiction de nombres aléatoires est définie comme un procédé rendant possible des attaques par force brute par la prédiction partielle ou totale de nombres générés aléatoirement.

SECTION IV

Menaces pour les portefeuilles

Cette dernière section présente une sélection de scénarios de menace classiques touchant spécifiquement les portefeuilles, qui sont mis en correspondance avec les principaux risques de haut niveau qui y sont liés et dont la liste figure ci-dessus. Cette liste indique les menaces à couvrir, mais ne constitue pas une liste de menaces exhaustive, qui est largement fonction de l'architecture de la solution de portefeuille retenue et de l'évolution de l'environnement de menace. En outre, dans l'évaluation des risques et les mesures proposées, le fournisseur de portefeuille ne peut être responsable que des composants relevant du champ d'application de la certification (*).

ID *Identifiant*	Description de la menace *Description de la menace identifiée (*)*	Intitulé du risque *Risques correspondants*
TR1	Un attaquant peut révoquer des pseudonymes sans motif justifié.	Création ou utilisation d'une fausse identité électronique (R2)
TR2	Un attaquant peut délivrer des identités électroniques fabriquées qui n'existent pas.	Création ou utilisation d'une fausse identité électronique (R2)
TR3	Un attaquant peut commencer à délivrer des PID non autorisées.	Création ou utilisation d'une fausse identité électronique (R2)
TR4	Un attaquant peut obtenir d'un administrateur qu'il saisisse un fournisseur de PID erroné dans la liste de confiance des fournisseurs de PID.	Création ou utilisation d'une fausse identité électronique (R2)
TR5	Un attaquant peut contourner le service de validation d'identité à distance.	Création ou utilisation d'une identité électronique existante (R1)/Création ou utilisation d'une fausse identité électronique (R2)
TR6	Un attaquant peut contourner le service de validation d'identité physique.	Création ou utilisation d'une identité électronique existante (R1)/Création ou utilisation d'une fausse identité électronique (R2)
TR7	Un attaquant peut contourner les services de validation d'identité liés à l'utilisation d'un certificat (qualifié) à distance.	Création ou utilisation d'une identité électronique existante (R1)/Création ou utilisation d'une fausse identité électronique (R2)
TR8	Un attaquant peut avoir accès à un portefeuille qui n'est pas lié à une personne.	Création ou utilisation d'une identité électronique existante (R1)/Création ou utilisation d'une fausse identité électronique (R2)
TR9	Un attaquant peut déjouer les contrôles techniques et procéduraux pour créer des PID erronées.	Création ou utilisation d'une identité électronique existante (R1)/Création ou utilisation d'une fausse identité électronique (R2)
TR10	Un attaquant peut activer un nouveau portefeuille sur un dispositif cryptographique sécurisé de portefeuille (WSCD) non valable.	Création ou utilisation d'une identité électronique existante (R1)/Création ou utilisation d'une fausse identité électronique (R2)
TR11	Un attaquant peut contourner les services de validation d'identité liés à l'utilisation de moyens d'identification électronique existants.	Création ou utilisation d'une identité électronique existante (R1)/Vol d'identité (R4)/Transaction non autorisée (R9)
TR12	Un attaquant peut contourner la vérification, par le fournisseur de PID, que le portefeuille se trouve sous le contrôle de l'utilisateur et faire en sorte qu'une PID soit délivrée dans un portefeuille compromis placé sous le contrôle de l'attaquant.	Création ou utilisation d'une identité électronique existante (R1)/Vol d'identité (R4)/Transaction non autorisée (R9)

ID *Identifiant*	Description de la menace *Description de la menace identifiée (*)*	Intitulé du risque *Risques correspondants*
TR13	Un attaquant peut obtenir une PID valable dans une unité de portefeuille non valable.	Création ou utilisation d'une identité électronique existante (R1)/Vol d'identité (R4)/Transaction non autorisée (R9)
TR14	Un fournisseur de PID peut délivrer des identités fabriquées dans une situation où l'identité est liée à une personne existante.	Création ou utilisation d'une identité électronique existante (R1)/Vol d'identité (R4)/Transaction non autorisée (R9)
TR15	Un attaquant peut lier une PID au portefeuille erroné parce que le fournisseur de PID n'est pas en mesure de relier la PID au bon portefeuille.	Création ou utilisation d'une identité électronique existante (R1)/Vol d'identité (R4)/Transaction non autorisée (R9)
TR16	Un attaquant peut faire approuver par l'utilisateur l'activation d'une nouvelle unité/instance de portefeuille placée sous le contrôle de l'attaquant, permettant également un contrôle ultérieur des attestations.	Création ou utilisation d'une identité électronique existante (R1)/Création ou utilisation d'une fausse identité électronique (R2)/Vol d'identité (R4)/Transaction non autorisée (R9)
TR17	Un attaquant peut émettre une PID d'un autre État pour accéder aux données/actifs numériques de citoyens ciblés.	Création ou utilisation d'une identité électronique existante (R1)/Vol d'identité (R4)/Transaction non autorisée (R9)
TR18	Un attaquant peut déjouer les contrôles techniques et procéduraux pour créer de fausses attestations électroniques d'attributs (qualifiées).	Création ou utilisation de faux attributs (R3)
TR19	Un attaquant peut présenter des attestations électroniques d'attributs (qualifiées) qui ne lui sont pas délivrées valablement.	Création ou utilisation de faux attributs (R3)
TR20	Un attaquant peut attaquer le mécanisme de liaison cryptographique du portefeuille entre la PID et une attestation électronique d'attributs (qualifiée) qui ne devrait pas lui être délivrée.	Création ou utilisation de faux attributs (R3)
TR21	Un attaquant peut utiliser une attestation électronique d'attributs (qualifiée) dans un portefeuille, bien que l'équivalent physique de celle-ci ait expiré ou ne soit pas valable.	Création ou utilisation de faux attributs (R3)
TR22	Un attaquant peut contourner la vérification, par le fournisseur d'attestation électronique d'attributs (qualifiée), que le portefeuille se trouve sous le contrôle de l'utilisateur et faire en sorte qu'une attestation électronique d'attributs (qualifiée) soit délivrée dans un portefeuille compromis placé sous le contrôle de l'attaquant.	Création ou utilisation de faux attributs (R3)
TR23	Un attaquant peut contrefaire des attestations électroniques d'attributs.	Création ou utilisation de faux attributs (R3)
TR24	Un attaquant peut injecter des attestations électroniques d'attributs contrefaites dans un portefeuille.	Création ou utilisation de faux attributs (R3)
TR25	Le portefeuille peut présenter des attributs à une partie utilisatrice sans l'approbation d'un utilisateur.	Divulgation de données (R6)
TR26	Les PID, les attestations électroniques d'attributs (qualifiées) ou les pseudonymes peuvent être présentés à une partie utilisatrice erronée.	Divulgation de données (R6)
TR27	Un attaquant peut lancer un renouvellement d'attestation électronique d'attributs malveillant.	Divulgation de données (R6)
TR28	Un attaquant peut obtenir d'un utilisateur qu'il approuve à tort une demande d'attestations électroniques d'attributs (hameçonnage ou autre).	Divulgation de données (R6)

ID *Identifiant*	Description de la menace *Description de la menace identifiée (*)*	Intitulé du risque *Risques correspondants*
TR29	Un attaquant peut divulguer des attributs du portefeuille et identifier l'utilisateur du portefeuille dans une situation où l'identification n'est pas requise/autorisée.	Divulgation de données (R6)
TR30	Un attaquant peut déjouer les contrôles techniques et procéduraux pour extraire des données.	Divulgation de données (R6)
TR31	Une demande peut être divulguée à un attaquant.	Divulgation de données (R6)
TR32	Un attaquant peut obtenir des informations sur la politique de divulgation intégrée en matière d'attributs et présenter des attributs contenus dans la demande en cours émanant des unités de portefeuille.	Divulgation de données (R6)
TR33	Un attaquant peut extraire des journaux, en totalité ou en partie.	Divulgation de données (R6)
TR34	Un attaquant peut savoir si un portefeuille est installé sur l'appareil qu'il utilise lui-même ou sur un autre appareil, et obtenir des informations à son sujet.	Divulgation de données (R6)
TR35	Un attaquant peut obtenir un facteur de connaissance utilisé pour l'authentification de l'utilisateur dans l'application cryptographique sécurisée de portefeuille (WSCA).	Divulgation de données (R6)
TR36	Le fait de présenter une attestation électronique d'attributs concernant une personne dans le cadre de transactions multiples avec une partie utilisatrice, ou entre différentes parties utilisatrices, permet, sans que cela soit intentionnel, de lier plusieurs transactions à la personne concernée.	Divulgation de données (R6)
TR37	Une liste publique de révocation d'attestations/de parties utilisatrices peut contenir des informations sur l'usage que fait l'utilisateur de son attestation (par exemple, localisation, adresse IP, etc.).	Divulgation de données (R6)
TR38	N'étant pas en mesure de prouver le consentement de l'utilisateur pour des attributs partagés, les parties utilisatrices peuvent porter atteinte à l'intégrité des journaux.	Divulgation de données (R6)
TR39	Un attaquant peut tracer illégalement des utilisateurs de portefeuille en utilisant des identifiants uniques/traçables.	Divulgation des données (R6)/Surveillance (R14)
TR40	Une partie utilisatrice composée de plusieurs unités/entités dont chacune possède un champ d'action différent quant à ce qu'elle est autorisée à demander/traiter peut demander et traiter des données sans y être légalement habilitée.	Divulgation des données (R6)/Transaction non autorisée (R9)
TR41	Un attaquant peut altérer les contrôles d'intégrité et d'authenticité effectués par le portefeuille de PID de manière à ce qu'ils renvoient systématiquement une réponse positive.	Manipulation de données (R7)
TR42	Un attaquant peut contourner ou altérer la réalisation des contrôles effectués par le portefeuille pour vérifier l'intégrité et l'authenticité des attributs demandés de manière à ce qu'ils renvoient systématiquement une réponse positive.	Manipulation de données (R7)
TR43	Un attaquant peut contourner ou altérer la réalisation des contrôles effectués par le portefeuille pour vérifier tous les attributs demandés qui appartiennent au même utilisateur de manière à ce qu'ils renvoient systématiquement une réponse positive.	Manipulation de données (R7)
TR44	Un attaquant peut contourner ou altérer la réalisation des contrôles effectués par le portefeuille pour vérifier si la PID est valable et délivrée par un fournisseur de PID de confiance de manière à ce qu'ils renvoient systématiquement une réponse positive.	Manipulation de données (R7)

ID *Identifiant*	Description de la menace *Description de la menace identifiée* (*)	Intitulé du risque *Risques correspondants*
TR45	Un attaquant peut contourner ou altérer la réalisation des contrôles effectués par le portefeuille pour vérifier qu'une attestation électronique d'attributs qualifiée est valable et délivrée par un prestataire de services de confiance qualifié, enregistré pour la délivrance de l'attestation électronique d'attributs qualifiée, de manière à ce qu'ils renvoient systématiquement une réponse positive.	Manipulation de données (R7)
TR46	Un attaquant peut contourner ou altérer la réalisation des contrôles effectués par le portefeuille pour vérifier si la PID a été révoquée par le fournisseur de PID de manière à ce qu'ils renvoient systématiquement une réponse positive.	Manipulation de données (R7)
TR47	Un attaquant peut contourner ou altérer la réalisation des contrôles effectués par le portefeuille pour vérifier si l'attestation électronique d'attributs (qualifiée) a été révoquée par le fournisseur d'attestations électroniques d'attributs (qualifiées) de manière à ce qu'ils renvoient systématiquement une réponse positive.	Manipulation de données (R7)
TR48	Un attaquant peut modifier le contenu de données de sauvegarde et de récupération qui devraient se trouver exclusivement sous le contrôle de l'utilisateur.	Manipulation de données (R7)/Perte de données (R8)
TR49	Un attaquant peut modifier l'historique des transactions pour une instance de portefeuille donnée à partir des journaux d'activité.	Manipulation de données (R7)/Perte de données (R8)
TR50	Un attaquant peut pratiquer des écoutes pendant la connexion du portefeuille aux parties utilisatrices.	Vol de données (R5)/Divulgation de données (R6)
TR51	Un attaquant peut convaincre un utilisateur de partager des données à caractère personnel (c'est-à-dire des PID, des attestations électroniques d'attributs, des pseudonymes, des signatures électroniques, des journaux et d'autres données) avec l'attaquant ou avec un tiers alors que l'utilisateur n'en avait pas l'intention.	Vol de données (R5)/Divulgation de données (R6)
TR52	Un attaquant peut lire l'historique des transactions pour une instance de portefeuille donnée à partir des journaux d'activité.	Vol de données (R5)/Divulgation de données (R6)
TR53	Un attaquant peut exporter ou extraire du matériel de clé cryptographique à partir du dispositif cryptographique sécurisé de portefeuille (WSCD).	Vol de données (R5)/Divulgation de données (R6)/Transaction non autorisée (R9)
TR54	Un attaquant peut lire le contenu de données de sauvegarde et de récupération qui devraient se trouver exclusivement sous le contrôle de l'utilisateur.	Vol de données (R5)/Divulgation de données (R6)
TR55	Un attaquant peut contourner la méthode d'authentification de l'utilisateur pour utiliser un pseudonyme généré par une unité de portefeuille.	Vol d'identité (R4)
TR56	Un attaquant peut proposer aux utilisateurs une application qui imite un portefeuille légitime spécifique.	Vol d'identité (R4)
TR57	Un attaquant peut exporter des données de portefeuille, y compris des PID, des attestations d'attributs électroniques (qualifiées) ou des journaux.	Vol d'identité (R4)
TR58	Un attaquant peut exporter du matériel de liaison cryptographique.	Vol d'identité (R4)
TR59	Un attaquant peut s'emparer d'identités au moyen des clés cryptographiques du portefeuille.	Vol d'identité (R4)
TR60	Un attaquant peut dupliquer l'unité de portefeuille personnelle d'un autre utilisateur sur son propre appareil et l'utiliser.	Vol d'identité (R4)/Création ou utilisation d'une identité électronique existante (R1)

ID *Identifiant*	Description de la menace *Description de la menace identifiée* (*)	Intitulé du risque *Risques correspondants*
TR61	Les autorités d'un autre État peuvent demander à l'utilisateur de montrer et/ou de partager toutes les données du portefeuille dans une situation de proximité, par exemple lors du franchissement de la frontière de cet État.	Vol d'identité (R4)/Surveillance (R14)
TR62	Les utilisateurs ne peuvent pas transférer leurs journaux de transactions après la défaillance d'un appareil utilisateur, ce qui entraîne une perte de traçabilité des transactions antérieures sur le nouveau portefeuille.	Répudiation (R11)
TR63	Les utilisateurs ne peuvent pas récupérer leurs journaux de transactions après la défaillance d'un appareil utilisateur, ce qui entraîne une perte de traçabilité sur le nouveau portefeuille.	Répudiation (R11)
TR64	Les parties utilisatrices peuvent éprouver des difficultés à prouver leur consentement aux signatures électroniques à distance.	Répudiation (R11)
TR65	Un attaquant peut inonder de demandes la ou les connexions lors de la connexion aux parties utilisatrices.	Interruption de service (R13)
TR66	Un attaquant peut inonder de connexions à des parties utilisatrices un service de fourniture de statut.	Interruption de service (R13)
TR67	Un attaquant peut faire apparaître comme contestée/refusée la présentation d'attributs, bien que celle-ci atteste sa validité.	Interruption de service (R13)
TR68	Un attaquant peut révoquer une PID sans motif justifié.	Interruption de service (R13)
TR69	Un attaquant peut révoquer une PID sans le consentement de l'utilisateur.	Interruption de service (R13)
TR70	Un attaquant peut révoquer une attestation électronique d'attributs (qualifiée) sans motif justifié.	Interruption de service (R13)
TR71	Un attaquant peut révoquer une attestation électronique d'attributs (qualifiée) sans le consentement de l'utilisateur.	Interruption de service (R13)
TR72	Un attaquant peut déclencher plusieurs demandes d'identification sans qu'elles soient reconnues comme des demandes orphelines intentionnelles.	Interruption de service (R13)
TR73	Un attaquant peut envoyer plusieurs demandes sans transaction de suivi.	Interruption de service (R13)
TR74	Un attaquant peut permettre à une partie utilisatrice de demander une identification sans identification (réponse) correspondante et contrôle total.	Interruption de service (R13)
TR75	Un attaquant peut envoyer une réponse à une demande après son expiration, ou situations similaires entraînant une interruption du service.	Interruption de service (R13)
TR76	Une partie utilisatrice peut envoyer plusieurs demandes non valables.	Interruption de service (R13)
TR77	Un attaquant peut envoyer plusieurs demandes non valables à un fournisseur de portefeuille.	Interruption de service (R13)
TR78	Un attaquant peut empêcher un État membre de révoquer un fournisseur de PID non fiable de la liste de confiance des fournisseurs de PID de confiance.	Interruption de service (R13)
TR79	Un attaquant peut empêcher la suspension ou la révocation d'un portefeuille.	Interruption de service (R13)

ID *Identifiant*	Description de la menace *Description de la menace identifiée (*)*	Intitulé du risque *Risques correspondants*
TR80	Un attaquant peut bloquer les transactions de parties utilisatrices, d'utilisateurs et/ou de fournisseurs de PID.	Interruption de service (R13)
TR81	Un attaquant peut désactiver ou rendre indisponible un dispositif cryptographique sécurisé de portefeuille (WSCD).	Interruption de service (R13)
TR82	Un attaquant peut empêcher le fournisseur de PID de révoquer ou de suspendre des PID.	Interruption de service (R13)/Transaction non autorisée (R9)
TR83	Une partie utilisatrice peut déduire les données d'identité de l'utilisateur au-delà des données qui lui sont communiquées.	Surveillance (R14)
TR84	Un groupe de parties utilisatrices ou de fournisseurs de PID qui sont de connivence peut déduire les données d'identité de l'utilisateur au-delà des données dont ce groupe a connaissance.	Surveillance (R14)
TR85	Un attaquant peut suivre et tracer un utilisateur en utilisant les données d'identification personnelle de celui-ci dans une situation où l'identification de l'utilisateur n'est pas requise.	Surveillance (R14)
TR86	Un attaquant peut assembler une présentation «contrefaite» de combinaisons d'attestations électroniques d'attributs (qualifiées).	Manipulation de transactions (R10)
TR87	Un attaquant peut activer le portefeuille ou s'en emparer à distance (par exemple, dans le cas d'une application bancaire intégrant une demande d'authentification ou d'attestation) sans le consentement exprès ou le contrôle exclusif de l'utilisateur, dans des situations où l'utilisateur n'a pas conscience de la partie utilisatrice (par exemple, s'il est endormi) ou ne peut pas la voir.	Manipulation de transactions (R10)
TR88	Les attaquants peuvent apporter des modifications aux métadonnées d'une demande (nom du service, utilisations, etc.).	Manipulation de transactions (R10)
TR89	Les attaquants peuvent apporter des modifications aux informations de la réponse (état du service, nonce, etc.).	Manipulation de transactions (R10)
TR90	Les attaquants peuvent apporter des modifications aux informations relatives aux attributs d'une demande (demandes surabondantes, etc.).	Manipulation de transactions (R10)
TR91	Une partie utilisatrice peut rejouer des éléments d'une session précédente lors d'une autre session.	Manipulation de transactions (R10)
TR92	Un attaquant peut remplacer ou modifier la PID pendant son transfert du fournisseur de PID à l'unité de portefeuille.	Manipulation de transactions (R10)
TR93	Un attaquant peut remplacer ou modifier la PID pendant son transfert de l'unité de portefeuille à la partie utilisatrice en ligne.	Manipulation de transactions (R10)
TR94	Un attaquant peut remplacer ou modifier la PID pendant son transfert de l'unité de portefeuille à la partie utilisatrice hors ligne.	Manipulation de transactions (R10)
TR95	Un attaquant peut délivrer une PID sans le consentement de l'utilisateur.	Transaction non autorisée (R9)
TR96	Un attaquant peut utiliser des politiques de divulgation intégrées révoquées ou non valables, éventuellement à l'insu des parties utilisatrices.	Transaction non autorisée (R9)
TR97	Un attaquant peut amener le portefeuille à déclarer valables des signatures électroniques erronées.	Transaction non autorisée (R9)
TR98	Un attaquant peut utiliser le portefeuille en dehors du contrôle de l'utilisateur.	Transaction non autorisée (R9)

ID *Identifiant*	Description de la menace *Description de la menace identifiée (*)*	Intitulé du risque *Risques correspondants*
TR99	Un attaquant peut convaincre un utilisateur d'authentifier et d'approuver des transactions avec un attaquant ou un tiers non autorisé.	Transaction non autorisée (R9)
TR100	Un attaquant peut faire signer électroniquement un utilisateur sans lui présenter le contenu ou après avoir présenté un contenu erroné.	Transaction non autorisée (R9)
TR101	Un attaquant peut contourner le contrôle d'accès du compte de l'utilisateur auprès du fournisseur de portefeuille.	Transaction non autorisée (R9)
TR102	Un attaquant peut usurper l'identité de parties utilisatrices lors de la connexion aux parties utilisatrices.	Transaction non autorisée (R9)/Divulgation de données (R6)
TR103	L'utilisateur au niveau de la connexion entre la partie utilisatrice et le navigateur peut être différent de l'utilisateur au niveau de la connexion entre la partie utilisatrice et le portefeuille.	Transaction non autorisée (R9)/Divulgation de données (R6)/Vol d'identité (R4)
TR104	Un attaquant peut convaincre l'utilisateur de révoquer son portefeuille sans raison.	Transaction non autorisée (R9)/Interruption de service (R13)
TR105	Un attaquant peut commettre des attaques de l'homme du milieu.	Transaction non autorisée (R9)/Divulgation de données (R6)/Surveillance d'identité (R14)
TR106	Un attaquant peut présenter des attributs non valables ou révoqués issus d'un portefeuille qui ne se connecte pas régulièrement au réseau.	Incidence sur différents risques
TR107	Un attaquant peut voler des informations à un utilisateur en usurpant un portefeuille.	Incidence sur différents risques
TR108	Un attaquant peut usurper l'identité de l'utilisateur en rejouant/en imitant une demande de données (par exemple, une authentification), qui semblerait valable.	Incidence sur différents risques
TR109	Un attaquant peut rejouer une politique de divulgation intégrée à l'intention d'un utilisateur, pour imiter une demande approuvée.	Incidence sur différents risques
TR110	Un attaquant peut exploiter le manque d'information des utilisateurs de portefeuille, ou les retards indus, à la suite d'une atteinte à la sécurité ou d'une altération.	Incidence sur différents risques
TR111	Un attaquant peut modifier un portefeuille légitime précédemment installé pour y ajouter des éléments malveillants.	Incidence sur différents risques
TR112	Un attaquant peut modifier une instance de portefeuille légitime et la proposer aux utilisateurs comme étant une instance légitime.	Incidence sur différents risques
TR113	Un attaquant peut déjouer le mécanisme même d'authentification de l'utilisateur pour contourner l'authentification de l'utilisateur de portefeuille.	Incidence sur différents risques
TR114	Un attaquant peut introduire du code malveillant ou des portes dérobées dans le code du portefeuille lors de son déploiement sur l'appareil de l'utilisateur.	Incidence sur différents risques
TR115	Un attaquant peut introduire du code malveillant ou des portes dérobées dans le code du portefeuille lors de son développement.	Incidence sur différents risques
TR116	Un attaquant peut manipuler frauduleusement la génération de nombres aléatoires afin de réduire suffisamment leur entropie pour permettre des attaques.	Incidence sur différents risques

ID *Identifiant*	Description de la menace *Description de la menace identifiée (*)*	Intitulé du risque *Risques correspondants*
TR117	Un attaquant peut manipuler frauduleusement des appareils d'utilisateurs dans la chaîne d'approvisionnement pour y inclure du code ou des configurations qui ne répondent pas aux conditions d'utilisation du portefeuille.	Incidence sur différents risques
TR118	Un attaquant peut activer une unité de portefeuille en utilisant par usurpation un dispositif cryptographique sécurisé de portefeuille (WSCD) contrôlé par les attaquants.	Incidence sur différents risques
TR119	Un attaquant peut lire les informations envoyées à l'application cryptographique sécurisée de portefeuille (WSCA) et/ou au dispositif cryptographique sécurisé de portefeuille (WSCD).	Incidence sur différents risques
TR120	Un attaquant peut envoyer des informations arbitraires à l'application cryptographique sécurisée de portefeuille (WSCA).	Incidence sur différents risques
TR121	Un attaquant peut voler des informations en interceptant des échanges entre l'application cryptographique sécurisée de portefeuille (WSCA) et/ou le dispositif cryptographique sécurisé de portefeuille (WSCD).	Incidence sur différents risques
TR122	Un attaquant peut envoyer des informations arbitraires au dispositif cryptographique sécurisé de portefeuille (WSCD).	Incidence sur différents risques
TR123	Un attaquant peut envoyer des informations au dispositif cryptographique sécurisé de portefeuille (WSCD) en contournant l'application cryptographique sécurisée de portefeuille (WSCA).	Incidence sur différents risques
TR124	Un attaquant peut utiliser l'hameçonnage pour diriger les utilisateurs vers une fausse application web de gestion de portefeuille et de PID.	Incidence sur différents risques
TR125	Un attaquant peut remplacer les clés d'un portefeuille par d'autres clés pour créer des messages à utiliser lors d'une autre attaque.	Incidence sur différents risques
TR126	Un attaquant peut modifier ou détruire les clés d'un portefeuille, rendant certaines fonctions du portefeuille inutilisables.	Incidence sur différents risques
TR127	Un attaquant peut contrôler un maliciel pour accéder aux données stockées dans le portefeuille.	Incidence sur différents risques
TR128	Un attaquant peut accéder à des éléments de preuve générés dans le portefeuille.	Incidence sur différents risques
TR129	Les fournisseurs de portefeuille peuvent accéder à des objets dans le portefeuille.	Incidence sur différents risques
TR130	Les fournisseurs de portefeuille peuvent accéder à des éléments de preuve générés dans le portefeuille.	Incidence sur différents risques
TR131	Un attaquant peut voler un dispositif de portefeuille déverrouillé.	Incidence sur les plusieurs risques
TR132	Un attaquant peut manipuler le système pour empêcher que certains événements ne soient journalisés.	Incidence sur différents risques
TR133	Un attaquant peut intercepter la communication entre l'instance de portefeuille et l'application cryptographique sécurisée de portefeuille (WSCA), ou rejouer/imiter un utilisateur (par exemple, en piratant le mécanisme d'authentification).	Incidence sur différents risques

ANNEXE II

CRITÈRES D'ÉVALUATION DE L'ACCEPTABILITÉ DES INFORMATIONS EN MATIÈRE DE GARANTIE

Dénomination	Objet	Points à vérifier
EUCC	Produits TIC	Concernant l'entité de délivrance: néant (organismes de certification accrédités) Concernant le champ d'application: — vérifier le profil de protection et la cible de sécurité — vérifier le niveau de garantie de l'évaluation et les augmentations Concernant la garantie: — vérifier les restrictions dans les documents destinés à l'utilisateur — pour la composition, l'accès au rapport technique d'évaluation peut être requis
EUCS (lorsqu'il est disponible)	Services en nuage	Concernant l'entité de délivrance: néant (organismes de certification accrédités) Concernant le champ d'application: — vérifier la description du service en nuage — vérifier le niveau d'évaluation et les profils d'extension Concernant la garantie: — vérifier les informations relatives à la transparence et, s'il y a lieu, les informations relatives à la composition
Schémas de critères communs utilisés dans l'UE, y compris les schémas SOG-IS	Produits TIC	Concernant l'entité de délivrance: néant (États membres) Concernant le champ d'application: — vérifier le profil de protection et la cible de sécurité — vérifier le niveau de garantie de l'évaluation et les augmentations Concernant la garantie: — vérifier les restrictions dans les documents destinés à l'utilisateur — pour la composition, l'accès au rapport technique d'évaluation peut être requis
EN 17640:2018 (FITCEM, y compris CSPN, BSZ, LINCE, BSZA)	Produits TIC	Concernant l'entité de délivrance: — vérifier le schéma et les exigences applicables aux organismes de certification Concernant le champ d'application: — vérifier la description du produit — vérifier les déclarations de sécurité — vérifier le niveau de garantie Concernant la garantie: — vérifier les activités réalisées et les constatations du rapport
Schémas de certification des dispositifs de création de signature qualifiés conformément à l'article 30 du règlement (UE) nº 910/2014	QSCD	Concernant l'entité de délivrance: — vérifier le schéma et les exigences applicables aux organismes de certification Concernant le champ d'application: — vérifier la description du produit — vérifier les déclarations de sécurité — vérifier le niveau de garantie Concernant la garantie: — vérifier les activités réalisées

Dénomination	Objet	Points à vérifier
EN ISO/IEC 27001:2022	ISMS	Concernant l'entité de délivrance: néant (organismes de certification accrédités) Concernant le champ d'application: — vérifier la description du système de gestion — vérifier la déclaration d'applicabilité Concernant la garantie: — vérifier les activités réalisées
SOC2	Organisations	Concernant l'entité de délivrance: — vérifier son statut d'expert-comptable Concernant le champ d'application: — vérifier la déclaration de gestion et la description des contrôles — vérifier la déclaration d'applicabilité Concernant la garantie: — vérifier les constatations figurant dans le rapport — vérifier les lettres de pont si nécessaire
MDSCert (GSMA) (si disponible)	Dispositifs mobiles	Concernant l'entité de délivrance: — vérifier les exigences applicables aux organismes de certification Concernant le champ d'application: — vérifier le niveau de garantie de sécurité — vérifier les exigences applicables au schéma Concernant la garantie: — vérifier les activités et les constatations figurant dans le rapport
Autres schémas	Tout composant	Concernant le schéma: — vérifier la pertinence et les dispositions du schéma Concernant l'entité de délivrance: — vérifier les exigences applicables aux organismes de certification Concernant le champ d'application: — vérifier les exigences applicables au schéma — vérifier la cible de sécurité ou le document similaire décrivant les exigences fonctionnelles et les exigences en matière de garantie de sécurité — vérifier la description du produit et une sélection d'exigences fonctionnelles de sécurité Concernant la garantie: — vérifier les activités et les constatations figurant dans le rapport

ANNEXE III

EXIGENCES FONCTIONNELLES POUR LES SOLUTIONS DE PORTEFEUILLE

En vertu de l'article 5 *bis*, paragraphes 4, 5, 8 et 14, du règlement (UE) n° 910/2014, les critères fonctionnels à remplir par une solution de portefeuille certifiée et le schéma d'identification électronique dans le cadre duquel elle est fournie comprennent les exigences fonctionnelles applicables aux opérations énumérées dans les actes suivants:

1) règlement d'exécution (UE) 2024/2979 de la Commission [1] portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne l'intégrité et les fonctionnalités essentielles;

2) règlement d'exécution (UE) 2024/2982 de la Commission [2] portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les protocoles et les interfaces que doit prendre en charge le cadre européen relatif à une identité numérique;

3) règlement d'exécution (UE) 2024/2977 de la Commission [3] portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les données d'identification personnelle et les attestations électroniques d'attributs délivrées aux portefeuilles européens d'identité numérique.

---

[1] Règlement d'exécution (UE) 2024/2979 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne l'intégrité et les fonctionnalités essentielles (JO L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

[2] Règlement d'exécution (UE) 2024/2982 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les protocoles et les interfaces que doit prendre en charge le cadre européen relatif à une identité numérique (JO L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

[3] Règlement d'exécution (UE) 2024/2977 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les données d'identification personnelle et les attestations électroniques d'attributs délivrées aux portefeuilles européens d'identité numérique (JO L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

ANNEXE IV

MÉTHODES ET PROCÉDURES APPLICABLES AUX ACTIVITÉS D'ÉVALUATION

1. **Audit de la mise en œuvre d'une solution de portefeuille**

Une activité d'évaluation de la conformité consiste à sélectionner des activités d'évaluation spécifiques.

Les schémas nationaux de certification spécifient une activité d'évaluation destinée à évaluer les informations fournies, couvrant au moins les éléments suivants:

a) une analyse des informations fournies pour confirmer qu'elles sont adaptées à l'une des architectures spécifiées dans les schémas nationaux de certification;

b) une analyse de la couverture des risques et menaces de cybersécurité recensés dans le registre des risques visé à l'annexe I par les contrôles de sécurité décrits.

L'analyse visée aux points a) et b) se fonde sur les motifs et la justification fournis par le fournisseur de portefeuille.

2. **Activités d'évaluation liées au dispositif cryptographique sécurisé de portefeuille (WSCD)**

1) Il n'est pas obligatoire que les opérations critiques, y compris les calculs cryptographiques, soient pleinement mises en œuvre dans le WSCD. Cependant, la partie mise en œuvre dans le WSCD, lorsqu'elle fonctionne comme un élément de la solution de portefeuille, garantit la protection des opérations critiques qu'elle effectue contre les attaques perpétrées par des attaquants ayant un potentiel d'attaque élevé conformément au règlement d'exécution (UE) 2015/1502 de la Commission ([1]).

2) Tout ou partie du WSCD peut être inclus dans l'objet de la certification lorsqu'il est fourni par le titulaire du certificat ou le demandeur, ou en être exclu lorsqu'il est intégré dans un dispositif fourni par l'utilisateur final. En outre, les schémas nationaux de certification spécifient les activités d'évaluation destinées à vérifier l'adéquation du WSCD, dans les deux cas suivants:

   a) si la WSCA dépend du WSCD considéré (c'est-à-dire si elle doit être évaluée en tant que produit composite basé sur le WSCD), l'évaluation de la WSCA requiert d'accéder à des informations supplémentaires relatives à la certification du WSCD, y compris, en particulier, son rapport technique d'évaluation;

   b) si une architecture envisagée dans le schéma utilise plusieurs WSCD, ou si certaines des opérations portant sur des actifs critiques sont réalisées en dehors du WSCD, les schémas nationaux de certification comprennent des activités d'évaluation destinées à garantir que la solution globale offre le niveau de sécurité attendu.

3) Comme condition préalable à la certification dans le cadre des schémas nationaux de certification, le WSCD est évalué au regard des exigences du niveau de garantie élevé énoncées dans le règlement d'exécution (UE) 2015/1502.

   Lorsque les conditions prévues à l'article 3, paragraphe 3, point b), sont remplies, l'évaluation de tout ou partie du WSCD comprend une évaluation de la vulnérabilité telle que définie dans la norme EN ISO/IEC 15408-3:2022 au niveau AVA_VAN.5, conformément à l'annexe I du règlement d'exécution (UE) 2024/482 de la Commission ([2]), sauf à justifier dûment auprès de l'organisme de certification que les caractéristiques de sécurité de la WSCA permettent d'utiliser un niveau d'évaluation inférieur tout en maintenant globalement le même niveau de garantie élevé que celui prévu dans le règlement d'exécution (UE) 2015/1502.

([1]) Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (JO L 235 du 9.9.2015, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

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

4) En outre, dans la documentation relative à chaque architecture spécifique, les schémas nationaux de certification formulent des hypothèses pour l'évaluation du WSCD en vertu de laquelle une résistance peut être offerte aux attaquants ayant un potentiel d'attaque élevé conformément au règlement d'exécution (UE) 2015/1502 et spécifient les activités d'évaluation destinées à confirmer ces hypothèses et à confirmer, après la délivrance du certificat, que les hypothèses sont toujours vérifiées. Les schémas nationaux exigent également des candidats à la certification qu'ils affinent ces hypothèses en fonction de leur mise en œuvre spécifique et qu'ils décrivent les mesures mises en place pour garantir que les hypothèses sont vérifiées tout au long du cycle de certification.

5) Dans tous les cas, les schémas nationaux de certification comprennent une activité d'évaluation destinée à vérifier que les informations en matière de garantie disponibles pour le WSCD sont adaptées aux fins de la solution de portefeuille en procédant à une analyse des informations en matière de garantie, telles que la cible de sécurité pour les certificats EUCC, comprenant les activités suivantes:

   a) vérifier que la portée de l'évaluation est appropriée, ce qui implique, pour les certificats EUCC, par exemple, de vérifier que les cibles de sécurité sont conformes à l'un des profils de protection recommandés dans l'EUCC;

   b) vérifier que les hypothèses relatives à l'environnement d'exploitation sont compatibles avec la solution de portefeuille, ce qui signifie, pour les certificats EUCC, par exemple, que ces hypothèses se retrouvent dans la cible de sécurité;

   c) vérifier que les recommandations figurant dans les consignes d'utilisation ou dans la documentation de l'utilisateur sont compatibles avec les conditions d'utilisation du WSCD dans la solution de portefeuille;

   d) vérifier que les hypothèses formulées dans le schéma national de certification concernant les WSCD sont vérifiées et couvertes par les informations en matière de garantie.

6) Dans les cas où certaines vérifications ne sont pas totalement concluantes, les schémas nationaux de certification exigent des organismes de certification qu'ils définissent des exigences de compensation pour l'application cryptographique sécurisée de portefeuille (WSCA) sur la base du WSCD, qui doivent figurer dans l'évaluation de la WSCA. À défaut, les schémas nationaux de certification considèrent que le WSCD n'est pas approprié, ce qui signifie que la solution de portefeuille ne reçoit pas de certificat de conformité.

3. **Activités d'évaluation liées à l'application cryptographique sécurisée de portefeuille (WSCA)**

1) Les schémas nationaux de certification exigent qu'une WSCA, dans le cadre d'une solution de portefeuille, soit évaluée au regard des exigences correspondant au minimum à un niveau de garantie élevé au sens du règlement d'exécution (UE) 2015/1502.

2) Cette évaluation comprend une évaluation de la vulnérabilité telle que définie dans la norme EN ISO/IEC 15408-3:2022 au niveau AVA_VAN.5, conformément à l'annexe I du règlement d'exécution (UE) 2024/482, sauf à justifier dûment auprès de l'organisme de certification que les caractéristiques de sécurité de la WSCA permettent d'utiliser un niveau d'évaluation inférieur tout en maintenant globalement le même niveau de garantie élevé que celui prévu dans le règlement d'exécution (UE) 2015/1502.

3) Lorsque la WSCA n'est pas fournie par le fournisseur de portefeuille, les schémas nationaux de certification formulent des hypothèses pour l'évaluation de la WSCA en vertu de laquelle une résistance peut être offerte aux attaquants ayant un potentiel d'attaque élevé conformément au règlement d'exécution (UE) 2015/1502 et spécifient les activités d'évaluation destinées à confirmer ces hypothèses et à confirmer, après la délivrance du certificat, que les hypothèses sont toujours vérifiées. Les schémas nationaux exigent également des candidats à la certification qu'ils affinent ces hypothèses en fonction de leur mise en œuvre spécifique et qu'ils décrivent les mesures mises en place pour garantir que les hypothèses sont vérifiées tout au long du cycle de certification.

4) Dans tous les cas, les schémas nationaux de certification comprennent une activité d'évaluation destinée à vérifier que les informations en matière de garantie disponibles pour la WSCA sont adaptées aux fins de la solution de portefeuille en procédant à une analyse des informations en matière de garantie, telles que la cible de sécurité pour les certificats EUCC, comprenant les activités suivantes:

   a) vérifier que la portée de l'évaluation est appropriée, ce qui implique, pour les certificats EUCC, par exemple, de vérifier que les cibles de sécurité sont conformes à l'un des profils de protection recommandés dans l'EUCC;

   b) vérifier que les hypothèses relatives à l'environnement d'exploitation sont compatibles avec la solution de portefeuille, ce qui signifie, pour les certificats EUCC, par exemple, que ces hypothèses se retrouvent dans la cible de sécurité;

c) vérifier que les recommandations figurant dans les consignes d'utilisation ou dans la documentation de l'utilisateur sont compatibles avec les conditions d'utilisation de la WSCA dans la solution de portefeuille;

d) vérifier que les hypothèses formulées dans le schéma national de certification concernant les WSCA sont vérifiées et couvertes par les informations en matière de garantie.

5) Les schémas nationaux de certification exigent que l'évaluation de la WSCA couvre tous les contrôles de sécurité mis en œuvre par cette WSCA.

4. **Activités d'évaluation liées à l'appareil de l'utilisateur final**

Étant donné que le registre des risques, tel qu'il est prévu à l'annexe I du présent règlement, recense les risques qui sont directement liés à la sécurité de l'appareil de l'utilisateur final, les schémas nationaux de certification définissent les exigences de sécurité applicables auxdits appareils. Toutefois, ces appareils étant fournis par l'utilisateur final et non par le fournisseur de portefeuille, ces exigences doivent être couvertes par des hypothèses.

Pour chaque hypothèse, la solution de portefeuille doit comporter un mécanisme permettant de vérifier, pour chaque unité de portefeuille, que l'appareil sous-jacent de l'utilisateur final satisfait à l'hypothèse. Ces mécanismes sont considérés comme des contrôles de sécurité et font l'objet d'activités d'évaluation destinées à démontrer à la fois leur adéquation et leur efficacité au niveau de garantie approprié.

En voici deux exemples:

a) un appareil d'utilisateur final peut comporter un WSCD certifié, cette certification devant être démontrée. Pour ce faire, il est classiquement fait usage d'un mécanisme cryptographique permettant de vérifier la présence, dans le WSCD certifié, d'un secret cryptographique qui est présent uniquement dans le WSCD certifié. Dans ce cas, ce secret cryptographique devrait être considéré comme un actif critique et être couvert par la certification du WSCD et/ou de la WSCA;

b) une exigence classique applicable aux appareils des utilisateurs finaux concerne l'obligation de procéder à des mises à jour de sécurité. Étant donné que cette exigence est liée à l'instance de portefeuille, le mécanisme utilisé pour vérifier la disponibilité des mises à jour de sécurité ne doit faire l'objet d'activités d'évaluation qu'à un niveau de garantie adapté à l'instance de portefeuille, d'autant plus qu'il est susceptible d'être intégré dans l'instance de portefeuille.

5. **Activités d'évaluation liées à l'instance de portefeuille**

1) L'évaluation de l'instance de portefeuille tient compte des deux grandes difficultés suivantes:

a) l'instance de portefeuille est susceptible de présenter un ensemble de variantes de la même application de base, chaque variante étant spécialisée pour une catégorie spécifique d'appareils d'utilisateur final;

b) les différentes variantes de l'instance de portefeuille nécessiteront probablement des mises à jour fréquentes afin de suivre le développement de la plateforme de sécurité sous-jacente, par exemple lorsque des vulnérabilités nécessitant des modifications des applications sont détectées.

2) L'évaluation de l'instance de portefeuille prend en considération ces difficultés spécifiques. L'une des conséquences immédiates est que le cadre des critères communs peut ne pas être approprié dans tous les cas. Par conséquent, d'autres méthodes d'évaluation sont envisagées s'il y a lieu. Les schémas nationaux de certification prévoient l'utilisation de la méthodologie EN 17640:2018 selon les modalités suivantes:

a) dans le cadre du schéma lui-même;

b) dans le cadre de schémas nationaux fondés sur la méthodologie;

c) dans le cadre de schémas nationaux fondés sur des principes similaires, mais créés avant l'élaboration de la méthodologie EN 17640:2018.

3) En outre, étant donné que la réalisation d'une évaluation spécifique complète de chaque variante peut présenter une valeur ajoutée limitée, les schémas nationaux de certification prévoient la définition de critères permettant la réalisation d'un échantillonnage, afin d'éviter la répétition d'activités d'évaluation identiques et de privilégier les activités spécifiques à une variante donnée. Les schémas nationaux de certification exigent de tous les organismes de certification qu'ils justifient leur recours à l'échantillonnage.

4) Les schémas nationaux de certification incluent les mises à jour de l'instance de portefeuille dans le processus global de gestion des changements défini pour la solution de portefeuille. Ils fixent également des règles relatives aux procédures à appliquer par le fournisseur de portefeuille pour chaque mise à jour (par exemple, l'analyse de l'incidence des modifications sur les contrôles de sécurité) et aux activités d'évaluation à effectuer par l'organisme de certification sur les mises à jour dans des conditions spécifiées (par exemple, l'évaluation de l'efficacité opérationnelle d'un contrôle de sécurité modifié). Le processus de gestion des modifications est l'un des processus dont l'efficacité opérationnelle doit être vérifiée chaque année conformément à l'article 18, paragraphe 3.

6. **Activités d'évaluation liées aux services et processus utilisés pour la fourniture et l'exploitation de la solution de portefeuille**

1) Aux fins de l'évaluation des services et processus qui jouent un rôle dans la fourniture et l'exploitation de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie, l'équipe d'évaluation recueille des éléments de preuve en menant des activités d'évaluation qui peuvent comprendre des activités d'audit, d'inspection, de vérification et de validation.

2) L'organisme de certification confirme que les éléments de preuve sont suffisants et appropriés pour offrir une garantie suffisante que les services et processus satisfont aux exigences de certification, en confirmant ce qui suit:

   a) l'exactitude des informations présentées dans la description des processus et des services;

   b) la pertinence de la conception et des contrôles des processus et des services pour répondre aux critères d'évaluation;

   c) l'efficacité opérationnelle de la mise en œuvre de ces contrôles sur l'ensemble d'une période déterminée avant l'évaluation.

3) L'exactitude de la description et l'efficacité opérationnelle d'une mise en œuvre des contrôles peuvent être considérées comme des objectifs de vérification, au sens de la norme ISO/IEC 17000:2020, des déclarations correspondantes du fournisseur de portefeuille (c'est-à-dire la confirmation de l'exactitude des événements qui se sont déjà produits ou des résultats déjà obtenus), tandis que la pertinence de la conception et des contrôles des services et processus pour répondre aux critères d'évaluation peut être considérée comme un objectif de validation, au sens de la norme ISO/IEC 17000:2020, de la déclaration correspondante du fournisseur de portefeuille (c'est-à-dire la confirmation de la plausibilité d'une utilisation future prévue ou du résultat prévu).

4) Étant donné que l'exploitation d'une solution de portefeuille n'est pas autorisée avant sa certification, l'efficacité opérationnelle ne peut pas être confirmée sur la base de l'exploitation effective de la solution. Par conséquent, elle doit être confirmée à l'aide d'éléments de preuve recueillis au cours d'essais ou de projets pilotes.

5) Des schémas nationaux de certification peuvent déjà exister pour des services et des processus spécifiques, par exemple pour l'enrôlement des utilisateurs. L'utilisation de ces schémas est prise en considération par les schémas nationaux de certification, le cas échéant.

7. **Activités d'évaluation liées aux services TIC utilisés pour la fourniture et l'exploitation de la solution de portefeuille**

1) Certaines architectures de portefeuille peuvent s'appuyer sur des services TIC dédiés, notamment des services en nuage pour la fourniture et l'exploitation d'une solution de portefeuille, et ces services peuvent héberger des données sensibles ainsi que des opérations sensibles. Dans ce cas, les schémas nationaux de certification définissent les exigences de sécurité applicables à ces services TIC.

2) Il existe déjà de nombreux schémas de certification pour les services TIC, les services en nuage et d'autres sources d'informations en matière de garantie, dont ceux énumérés à l'annexe II. Les schémas nationaux de certification s'appuient, lorsqu'ils sont disponibles et applicables, sur ces mécanismes existants, en recourant à l'un des mécanismes suivants:

   a) imposer l'utilisation d'un schéma spécifique ou d'une sélection de schémas, en définissant les conditions d'évaluation des services TIC ou des services en nuage à l'aide de ces schémas;

   b) laisser le choix de l'évaluation au fournisseur de portefeuille et utiliser l'activité d'analyse des dépendances pour déterminer si les informations en matière de garantie obtenues dans le cadre de ces évaluations sont appropriées.

3) Dans les deux cas, les schémas nationaux de certification définissent les activités d'évaluation supplémentaires nécessaires pour analyser ou compléter les informations obtenues dans le cadre de ces schémas.

ANNEXE V

LISTE DES INFORMATIONS ACCESSIBLES AU PUBLIC SUR LES PORTEFEUILLES

1. Les informations qui sont rendues publiques en vertu de l'article 8, paragraphe 5, comprennent au moins les éléments suivants:

   a) les limitations éventuelles de l'utilisation d'une solution de portefeuille;

   b) des orientations et des recommandations du fournisseur de portefeuille pour aider les utilisateurs finaux à assurer, de façon sécurisée, la configuration, l'installation, le déploiement, le fonctionnement et la maintenance des portefeuilles;

   c) la période pendant laquelle une assistance en matière de sécurité sera offerte aux utilisateurs finaux, en particulier en ce qui concerne la disponibilité de mises à jour liées à la cybersécurité;

   d) les coordonnées du fabricant ou du fournisseur et les méthodes acceptées pour recevoir des informations concernant des vulnérabilités de la part d'utilisateurs finaux et de chercheurs dans le domaine de la sécurité;

   e) une mention relative aux répertoires en ligne recensant les vulnérabilités publiquement divulguées liées aux portefeuilles ainsi que tout conseil pertinent en matière de cybersécurité.

2. Les informations visées au paragraphe 1 sont mises, de manière claire, complète et facilement accessible, dans un espace accessible au public, à la disposition de toute personne souhaitant utiliser une solution de portefeuille.

ANNEXE VI

MÉTHODE D'ÉVALUATION DE L'ACCEPTABILITÉ DES INFORMATIONS EN MATIÈRE DE GARANTIE

1. Évaluation de la disponibilité des documents relatifs à la garantie

Les évaluateurs établissent la liste des documents relatifs à la garantie qui sont disponibles pour chaque composant pertinent de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie. Ensuite, les évaluateurs apprécient la pertinence globale de chaque document relatif à la garantie pour l'examen des dépendances.

Les aspects suivants sont pris en compte dans l'analyse:

1) en ce qui concerne les documents relatifs à la garantie proprement dits:

   a) le type de documents relatifs à la garantie, avec tous les détails requis, (il s'agit, par exemple, de certificats de conformité répondant à la norme EN ISO/IEC 27001:2022 ou des types 1 ou 2 pour les rapports ISAE);
   b) la période couverte ou la durée de validité, cette période pouvant être complétée par une lettre de pont (un document couvrant une période comprise entre la date de fin de la période de référence du rapport ISAE courant et la publication d'un nouveau rapport ISAE) ou une déclaration similaire);
   c) le cadre applicable (par exemple, une norme existante);

   d) l'information selon laquelle les documents relatifs à la garantie comprennent ou non une mise en correspondance avec les exigences du schéma;

2) en ce qui concerne les compétences professionnelles et l'impartialité de l'entité dont émane le rapport de garantie:

   a) le nom de l'organisme de certification et, s'il est disponible, le nom de l'évaluateur principal;

   b) la preuve de la compétence de l'organisme de certification et de l'évaluateur (par exemple, accréditation, certification personnelle, etc.);

   c) la preuve de l'impartialité de l'organisme de certification et de l'évaluateur (par exemple, accréditation, etc.).

2. Évaluation de la garantie liée aux exigences individuelles

Les évaluateurs vérifient que les documents relatifs à la garantie disponibles pour la solution de portefeuille et le schéma d'identification électronique dans le cadre duquel elle est fournie sont suffisants pour établir que la solution de portefeuille répond aux attentes par rapport aux exigences individuelles du schéma de certification.

Cette évaluation est effectuée pour chaque composant pertinent de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie, en formulant une hypothèse sur les contrôles de sécurité de la solution de portefeuille.

Pour chacune de ces hypothèses, l'équipe d'évaluation détermine si la garantie fournie dans les documents relatifs à la garantie disponibles est suffisante ou non.

La détermination du caractère suffisant de la garantie repose sur les éléments suivants:

1) les informations requises sont disponibles, avec le niveau de garantie voulu, dans les documents relatifs à la garantie;

2) les informations disponibles dans les documents relatifs à la garantie ne couvrent pas l'intégralité du champ d'application de l'exigence, mais des contrôles supplémentaires ou des contrôles de compensation (c'est-à-dire des contrôles internes qui réduisent le risque de faiblesse effective ou potentielle des contrôles) mis en œuvre dans la solution de portefeuille ou dans le schéma d'identification électronique dans le cadre duquel elle est fournie permettent aux évaluateurs d'établir que les informations sont suffisantes;

3) les informations disponibles dans les documents relatifs à la garantie n'offrent pas le niveau de garantie voulu, mais les contrôles mis en œuvre pour évaluer et contrôler le fournisseur de portefeuille permettent aux évaluateurs d'établir que les informations sont suffisantes;

4) si les documents relatifs à la garantie mentionnent des défauts de conformité dans la conception ou la mise en œuvre des contrôles utilisés pour répondre à une hypothèse, les mesures correctives proposées et mises en œuvre par le fournisseur de portefeuille et examinées par ses évaluateurs sont suffisantes pour garantir qu'il est répondu à l'hypothèse.

ANNEXE VII

CONTENU DU CERTIFICAT DE CONFORMITÉ

1. Un identifiant unique attribué par l'organisme de certification délivrant le certificat de conformité.

2. Des informations relatives à la solution de portefeuille certifiée et aux schémas d'identification électronique dans le cadre desquels elle est fournie, ainsi qu'au titulaire du certificat de conformité, comprenant les informations suivantes:
   a) le nom de la solution du portefeuille;
   b) le nom des schémas d'identification électronique dans le cadre desquels la solution de portefeuille est fournie;
   c) la version de la solution de portefeuille qui a été évaluée;
   d) le nom, l'adresse et les coordonnées du titulaire du certificat de conformité;
   e) un lien vers le site web du titulaire du certificat de conformité contenant les informations qui doivent être mises à la disposition du public.

3. Des informations relatives à l'évaluation et à la certification de la solution de portefeuille et des schémas d'identification électronique en vertu desquels elle est fournie, comprenant les informations suivantes:
   a) le nom, l'adresse et les coordonnées de l'organisme de certification qui a délivré le certificat de conformité;
   b) s'il diffère de l'organisme de certification, le nom de l'organisme d'évaluation de la conformité qui a effectué l'évaluation, ainsi que les informations concernant son accréditation;
   c) le nom du propriétaire du schéma;
   d) les références au règlement (UE) n° 910/2014 et au présent règlement;
   e) une référence au rapport de certification associé au certificat de conformité;
   f) une référence au rapport d'évaluation de la certification associé au certificat de conformité;
   g) une référence aux normes utilisées pour l'évaluation, y compris leurs versions;
   h) la date de délivrance du certificat de conformité;
   i) la période de validité du certificat de conformité.

ANNEXE VIII

CONTENU DU RAPPORT PUBLIC DE CERTIFICATION ET DU RAPPORT D'ÉVALUATION DE LA CERTIFICATION

1. Le certificat public de certification comporte au minimum les éléments suivants:

   a) un résumé;

   b) l'identification de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie;

   c) une description de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel elle est fournie;

   d) les informations de sécurité à mettre à la disposition du public, comme décrit à l'annexe V, ou un renvoi à ces informations;

   e) un résumé du plan préliminaire d'audit et de validation;

   f) un résumé de l'examen et de la décision de certification.

2. Le rapport d'évaluation de la certification contient au moins:

   a) une description de la conception de la solution de portefeuille, du schéma d'identification et du processus d'enrôlement, ainsi que l'évaluation des risques et le plan de validation spécifique;

   b) une description de la manière dont la solution de portefeuille satisfait aux exigences prévoyant un niveau de garantie élevé et de la manière dont ce respect des exigences est démontré par les résultats de l'évaluation de la certification de la solution de portefeuille effectuée conformément au présent règlement;

   c) une description du résultat de l'évaluation de la conformité de la solution de portefeuille et du schéma d'identification électronique dans le cadre duquel les unités de portefeuille correspondantes sont fournies, en particulier la conformité aux éléments suivants:

      — les exigences fixées à l'article 5 *bis*, paragraphes 4, 5 et 8, du règlement (UE) n° 910/2014,

      — l'exigence de séparation logique énoncée à l'article 5 *bis*, paragraphe 14, du règlement (UE) n° 910/2014,

      — le cas échéant, les normes et spécifications techniques visées à l'article 5 *bis*, paragraphe 24, du règlement (UE) n° 910/2014, en décrivant le lien entre ces exigences et les exigences normatives correspondantes spécifiées par les schémas nationaux de certification;

   d) un résumé du résultat de l'exécution du plan de validation, comprenant tous les défauts de conformité constatés.

ANNEXE IX

CALENDRIER DES ÉVALUATIONS DE SURVEILLANCE OBLIGATOIRES

1. L'article 18 précise les exigences applicables au cycle de vie de la certification, en particulier la réalisation d'activités d'évaluation régulières. Ces activités comprennent au moins les éléments suivants:

   a) une évaluation complète de l'objet de l'évaluation de la conformité dans l'évaluation initiale et lors de chaque évaluation de recertification, comprenant une mise à jour de tout composant du produit;

   b) une évaluation de la vulnérabilité dans l'évaluation initiale et lors de chaque évaluation de recertification, et au moins tous les deux ans dans les évaluations de surveillance, couvrant au moins les changements intervenus dans l'objet de l'évaluation de la conformité et les changements intervenus dans l'environnement de menace depuis la dernière évaluation de la vulnérabilité;

   c) des activités supplémentaires telles que des tests d'intrusion en cas d'augmentation du niveau de risque ou d'apparition de nouvelles menaces;

   d) une évaluation de l'efficacité opérationnelle des processus de maintenance au moins une fois par an dans les évaluations de surveillance et de recertification, couvrant au moins les processus de contrôle des versions, de mise à jour et de gestion de la vulnérabilité;

   e) à la suite d'un examen concluant et d'une décision de certification, la délivrance d'un certificat de conformité après l'évaluation initiale et après chaque évaluation de recertification.

2. Un calendrier de référence est fourni dans le tableau 1 sur la base d'un cycle de 4 ans, dans lequel:

   a) l'année 1 commence à la première délivrance du certificat de conformité; et

   b) toutes les activités d'évaluation sont réalisées dans un délai de 12 mois à compter de l'évaluation de l'année précédente.

3. Le calendrier figurant dans le tableau 1 est une recommandation visant à garantir une recertification en temps utile et à éviter les perturbations dans la fourniture de la solution du portefeuille. D'autres calendriers sont envisageables, pour autant que la validité du certificat de conformité ne dépasse pas cinq ans, comme le prévoit l'article 5 *quater*, paragraphe 4, du règlement (UE) nº 910/2014.

4. Outre les évaluations régulières, une évaluation spéciale peut être déclenchée à la demande de l'organisme de certification ou du titulaire du certificat de conformité, à la suite d'une modification importante de l'objet de la certification ou de l'environnement de menace.

5. Toute évaluation, y compris les évaluations de surveillance et les évaluations spéciales, pourrait conduire à la délivrance d'un nouveau certificat de conformité, en particulier en cas de modifications importantes de l'objet de la certification, mais avec la même date d'expiration que le certificat de conformité initial.

Tableau 1

Un cycle d'évaluation complet de 4 ans

Temps	Type d'éval.	Activités
Année 0	Initiale	— Évaluation complète de l'objet de la certification, comprenant l'évaluation de la vulnérabilité — — Y compris une fonction permettant d'effectuer des mises à jour sur chaque composant logiciel — Évaluation des processus de maintenance, à l'exclusion de leur efficacité opérationnelle — Délivrance du certificat de conformité et début du cycle de 4 ans
Année 1	Surveillance	— Évaluation de l'efficacité opérationnelle des processus de maintenance — — Au moins contrôle de version, mise à jour, gestion de la vulnérabilité — Évaluation des modifications ayant une incidence sur la sécurité du produit

Temps	Type d'éval.	Activités
Année 2	Surveillance	— Évaluation de la vulnérabilité de la solution complète — Évaluation de l'efficacité opérationnelle des processus de maintenance — Au moins contrôle de version, mise à jour, gestion de la vulnérabilité — Évaluation des modifications ayant une incidence sur la sécurité du produit
Année 3	Surveillance	— Évaluation de l'efficacité opérationnelle des processus de maintenance — Au moins contrôle de version, mise à jour, gestion de la vulnérabilité — Évaluation des modifications ayant une incidence sur la sécurité du produit
Année 4	Recertification	1) Évaluation complète de l'objet de la certification, comprenant l'évaluation de la vulnérabilité 2) Évaluation simplifiée des éléments/processus qui n'ont pas été modifiés 3) Y compris une fonction permettant d'effectuer des mises à jour sur chaque composant logiciel 4) Évaluation des processus de maintenance, y compris leur efficacité opérationnelle 5) Délivrance d'un nouveau certificat de conformité