Journal officiel
de l'Union européenne

FR
Série L

2024/2979

4.12.2024

RÈGLEMENT D'EXÉCUTION (UE) 2024/2979 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 l'intégrité et les fonctionnalités essentielles 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 *bis*, paragraphe 23,

considérant ce qui suit:

(1) Le cadre européen relatif à une identité numérique établi par le règlement (UE) nº 910/2014 est un élément essentiel pour la mise en place d'un écosystème d'identité numérique sécurisé et interopérable dans l'ensemble de l'Union. Avec pour pierre angulaire les portefeuilles européens d'identité numérique (ci-après les «portefeuilles»), il vise à faciliter l'accès aux services dans l'ensemble des États membres, pour les personnes physiques et morales, tout en garantissant la protection des données à caractère personnel et le respect de la vie privée.

(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) L'article 5 *bis*, paragraphe 23, du règlement (UE) nº 910/2014 charge la Commission d'établir, au besoin, les spécifications et les procédures applicables. À cette fin, quatre règlements d'exécution ont été prévus en ce qui concerne les protocoles et les interfaces: règlement d'exécution (UE) 2024/2982 de la Commission ([4]), l'intégrité et les fonctionnalités essentielles: règlement d'exécution (UE) 2024/2979 de la Commission ([5]), les données d'identification personnelle et les attestations électroniques d'attributs: règlement d'exécution (UE) 2024/2977 de la Commission ([6]), ainsi que les notifications à la Commission: règlement d'exécution (UE) 2024/2980 de la Commission ([7]). Le présent règlement établit les exigences applicables concernant l'intégrité et les fonctionnalités essentielles des portefeuilles européens d'identité numérique.

([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]) Règlement d'exécution (UE) 2024/2982 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 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).

([5]) Règlement d'exécution (UE) 2024/2979 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 l'intégrité et les fonctionnalités essentielles des portefeuilles européens d'identité numérique (JO L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([6]) Règlement d'exécution (UE) 2024/2977 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 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).

([7]) Règlement d'exécution (UE) 2024/2980 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 les notifications relatives à l'écosystème des portefeuilles européens d'identité numérique transmises à la Commission (JO L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) La Commission évalue régulièrement les 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 ([8]), et en particulier sur l'architecture et le cadre de référence. Conformément au considérant 75 du règlement (UE) 2024/1183 du Parlement européen et du Conseil ([9]), 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 générales, l'architecture et le cadre de référence et de suivre les meilleures pratiques sur le marché intérieur.

(5) Afin de garantir une communication précise, une différenciation technique et une répartition claire des responsabilités, il est nécessaire d'établir une distinction entre les différents composants et configurations des portefeuilles. On entend par «solution de portefeuille» le système complet, fourni par un fournisseur de portefeuille, qui est nécessaire pour utiliser un portefeuille. Elle devrait comprendre les composants logiciels et matériels, ainsi que les services, paramètres et configurations nécessaires pour assurer le bon fonctionnement du portefeuille. Une solution de portefeuille peut être implantée sur les dispositifs et dans les environnements des utilisateurs ainsi que sur la structure dorsale du fournisseur. On entend par «unité de portefeuille» une configuration spécifique de la solution de portefeuille pour un utilisateur donné. Elle devrait comprendre l'application installée sur l'appareil ou dans l'environnement de l'utilisateur de portefeuille avec laquelle celui-ci interagit directement (l'«instance de portefeuille») et les éléments de sécurité nécessaires pour protéger les données et les transactions des utilisateurs. Ces éléments de sécurité devraient faire appel à des logiciels ou du matériel spécialement conçus pour chiffrer et sauvegarder les informations sensibles. Une instance de portefeuille devrait faire partie de l'unité de portefeuille et permettre à l'utilisateur de portefeuille d'accéder aux fonctionnalités de son portefeuille.

(6) La présence d'applications cryptographiques sécurisées de portefeuille en tant que composants spécialisés distincts au sein d'une unité de portefeuille est nécessaire pour assurer non seulement la protection des actifs critiques, tels que les clés cryptographiques privées, mais aussi la fourniture de fonctionnalités essentielles, telles que la présentation d'attestations électroniques d'attributs. L'utilisation de spécifications techniques communes peut faciliter l'accès des fournisseurs de portefeuilles aux éléments sécurisés intégrés. Les applications cryptographiques sécurisées de portefeuille peuvent être fournies de différentes manières et à divers types de dispositifs cryptographiques sécurisés de portefeuille. Lorsque des fournisseurs de portefeuille fournissent des applications cryptographiques sécurisées de portefeuille personnalisées sous la forme d'appliquettes Java Card à des éléments sécurisés intégrés, les fournisseurs de portefeuille devraient respecter les normes énumérées à l'annexe I ou des spécifications techniques équivalentes.

(7) Les unités de portefeuille devraient permettre aux fournisseurs de données d'identification personnelle ou d'attestations électroniques d'attributs de vérifier qu'ils délivrent ces données ou ces attestations à d'authentiques unités de portefeuille de l'utilisateur de portefeuille.

(8) Afin de garantir la protection des données dès la conception et par défaut, les portefeuilles devraient être dotés des techniques de protection de la vie privée les plus récentes. Ces caractéristiques/éléments devraient permettre l'utilisation des portefeuilles sans que l'utilisateur du portefeuille puisse être suivi d'une partie utilisatrice du portefeuille à l'autre, en fonction du scénario d'utilisation éventuel. Par exemple, les fournisseurs de portefeuille devraient envisager des mesures d'atténuation des risques pour la vie privée à la pointe de la technologie en ce qui concerne les attestations d'unités de portefeuille, telles que l'utilisation d'attestations d'unités de portefeuille éphémères ou la délivrance par lots. En outre, les politiques de divulgation intégrées devraient mettre en garde les utilisateurs de portefeuille contre la divulgation inappropriée ou illégale d'attributs provenant d'attestations électroniques d'attributs.

(9) Les attestations d'unités de portefeuille devraient permettre aux parties utilisatrices de portefeuille qui demandent des attributs à des unités de portefeuille de vérifier le statut de validité de l'unité de portefeuille avec laquelle elles communiquent, étant donné que les attestations d'unités de portefeuille doivent être révoquées lorsqu'une unité de portefeuille n'est plus considérée comme valable. Les informations relatives à l'état de validité des unités de portefeuille devraient être mises à disposition de manière interopérable, afin qu'elles puissent être utilisées par toutes les parties utilisatrices de portefeuille. En outre, dans les cas où les utilisateurs de portefeuille ont perdu leur unité de portefeuille ou n'en possèdent plus le contrôle, les fournisseurs de portefeuille devraient permettre aux utilisateurs de portefeuille de demander la révocation de leur unité de portefeuille. Afin de garantir le respect de la vie privée et la non-associabilité, les États membres devraient également utiliser des techniques de protection de la vie privée pour l'attestation d'unité de portefeuille. Il peut s'agir, par exemple, d'utiliser plusieurs attestations d'unité de portefeuille à différentes fins en divulguant uniquement les informations le plus strictement nécessaires sur le portefeuille pour assurer une transaction, ou de limiter la durée de vie de l'attestation d'unité de portefeuille au lieu de recourir à des identifiants de révocation.

([8]) JO L 210 du 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 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).

(10) Afin de garantir que tous les portefeuilles sont techniquement capables de recevoir et de présenter des données d'identification personnelle et des attestations électroniques d'attributs dans des scénarios transfrontières sans compromettre l'interopérabilité, les portefeuilles devraient prendre en charge des types prédéterminés de formats de données et permettre une divulgation sélective. Ainsi qu'il est précisé dans le règlement (UE) nº 910/2014, la divulgation sélective est un concept permettant au propriétaire des données de ne divulguer que certaines parties d'un ensemble de données plus large, afin que l'entité destinataire n'obtienne que les informations qui sont nécessaires pour la fourniture d'un service demandé par un utilisateur. Étant donné que les portefeuilles doivent permettre à l'utilisateur de divulguer les attributs de manière sélective, les normes énumérées à l'annexe II devraient être mises en œuvre de manière à offrir cette fonctionnalité des portefeuilles. En outre, les portefeuilles peuvent prendre en charge d'autres formats et fonctionnalités pour des cas d'utilisation spécifiques.

(11) La journalisation des transactions est un outil important pour assurer la transparence, dans la mesure où elle offre une vue d'ensemble des transactions à l'utilisateur du portefeuille. De plus, les journaux devraient être utilisés pour permettre le partage rapide et facile de certaines informations, à la demande de l'utilisateur de portefeuille, avec les autorités de contrôle compétentes instituées en vertu de l'article 51 du règlement (UE) 2016/679, en cas de comportement suspect des parties utilisatrices de portefeuille.

(12) Pour qu'un utilisateur de portefeuille puisse signer électroniquement, il convient de lui délivrer un certificat qualifié lié à un dispositif de création de signature électronique qualifié. L'utilisateur de portefeuille devrait avoir accès à une application de création de signature. Si la délivrance de certificats qualifiés est un service fourni par les prestataires de services de confiance qualifiés, les autres composants devraient pouvoir être fournis par les fournisseurs de portefeuille ou d'autres entités. Par exemple, les dispositifs de création de signature électronique qualifiés peuvent être gérés par des prestataires de services de confiance qualifiés sous la forme d'un service ou peuvent être localisés dans l'appareil de l'utilisateur de portefeuille, par exemple sous la forme d'une carte à puce. De même, les applications de création de signature peuvent être intégrées dans l'instance de portefeuille, constituer une application distincte sur l'appareil de l'utilisateur de portefeuille ou être fournies à distance.

(13) Les objets dédiés à l'exportation et à la portabilité des données peuvent journaliser les données d'identification personnelle et les attestations électroniques d'attributs qui ont été délivrées à une unité de portefeuille donnée. Ces objets permettent aux utilisateurs de portefeuille d'extraire les données pertinentes de leur unité de portefeuille afin de renforcer leur droit à la portabilité des données. Les fournisseurs de portefeuille sont encouragés à utiliser les mêmes solutions techniques pour mettre en œuvre également des processus de sauvegarde et de récupération pour les unités de portefeuille, permettant ainsi de récupérer des unités de portefeuille perdues ou de transférer des informations d'un fournisseur de portefeuille à un autre, s'il y a lieu et dans la mesure où cela peut se faire sans porter atteinte au droit à la protection des données et à la sécurité de l'écosystème d'identité numérique.

(14) La création de pseudonymes spécifiques pour les parties utilisatrices de portefeuille devrait permettre aux utilisateurs de portefeuille de s'authentifier sans fournir d'informations superflues aux parties utilisatrices de portefeuille. Comme le prévoit le règlement (UE) nº 910/2014, les utilisateurs de portefeuille doivent pouvoir accéder aux services en utilisant un pseudonyme, sauf en cas d'obligation légale d'utiliser l'identité juridique pour s'authentifier. Par conséquent, les portefeuilles devraient comporter une fonctionnalité permettant de générer des pseudonymes choisis et gérés par l'utilisateur pour s'authentifier lorsqu'ils accèdent à des services en ligne. La mise en œuvre des spécifications énoncées à l'annexe V devrait permettre d'assurer ces fonctionnalités en conséquence. En outre, les parties utilisatrices de portefeuille doivent s'abstenir de demander aux utilisateurs de fournir d'autres données que celles qui correspondent à l'utilisation prévue des portefeuilles dans le registre des parties utilisatrices. Les utilisateurs de portefeuille devraient pouvoir vérifier à tout moment les données d'enregistrement des parties utilisatrices.

(15) Comme le prévoit le règlement (UE) 2024/1183, les États membres ne devraient pas limiter, directement ou indirectement, l'accès aux services publics ou privés des personnes physiques ou morales qui ne choisissent pas d'utiliser des portefeuilles et devraient mettre à disposition des solutions de substitution appropriées.

(16) 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 ([10]) et a rendu son avis le 30 septembre 2024.

([10]) 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) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(17) Les mesures prévues par le présent règlement sont conformes à l'avis du comité visé à l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet et champ d'application

Le présent règlement établit les règles relatives à l'intégrité et aux fonctionnalités essentielles des portefeuilles, qui sont mises à jour régulièrement pour tenir compte de l'évolution des technologies et des normes ainsi que des travaux réalisés sur la base de la recommandation (UE) 2021/946, dont l'architecture et le cadre de référence.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

1) «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;

2) «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/éléments cryptographiques sécurisés de portefeuille fournie à un utilisateur de portefeuille donné par un fournisseur de portefeuilles;

3) «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 à utiliser l'unité de portefeuille serait très sérieusement affaiblie si leur disponibilité, leur confidentialité ou leur intégrité étaient compromises;

4) «fournisseur de données d'identification personnelle»: une personne physique ou morale chargée de délivrer et de révoquer les données d'identification personnelle et de veiller à ce que les données d'identification personnelle d'un utilisateur soient cryptographiquement liées à une unité de portefeuille;

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

6) «partie utilisatrice de portefeuille»: une partie utilisatrice qui a l'intention de se fier à des unités de portefeuille pour fournir des services publics ou privés au moyen d'une interaction numérique;

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

8) «attestation d'unité de portefeuille»: un objet de données qui décrit les composants de l'unité de portefeuille ou permet l'authentification et la validation de ces composants;

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

10) «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;

11) «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;

12) «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;

13) «opération cryptographique de portefeuille»: un mécanisme cryptographique nécessaire dans le cadre de l'authentification de l'utilisateur du portefeuille et de la délivrance ou présentation de données d'identification personnelle ou d'attestations électroniques d'attributs;

14) «certificat d'accès de partie utilisatrice de portefeuille»: un certificat de cachet électronique ou de signature électronique authentifiant et validant la partie utilisatrice de portefeuille, délivré par un fournisseur de certificats d'accès de partie utilisatrice de portefeuille;

15) «fournisseur de certificats d'accès de partie utilisatrice de portefeuille»: une personne physique ou morale mandatée par un État membre pour délivrer des certificats d'accès de partie utilisatrice aux parties utilisatrices de portefeuille enregistrées dans cet État membre.

CHAPITRE II

INTÉGRITÉ DES PORTEFEUILLES EUROPÉENS D'IDENTITÉ NUMÉRIQUE

Article 3

Intégrité de l'unité de portefeuille

1. Les unités de portefeuille n'exécutent aucune des fonctionnalités énumérées à l'article 5 *bis*, paragraphe 4, du règlement (UE) n° 910/2014, sauf l'authentification de l'utilisateur de portefeuille pour accéder à l'unité de portefeuille, tant que l'unité de portefeuille n'a pas authentifié l'utilisateur du portefeuille.

2. Pour chaque unité de portefeuille, les fournisseurs de portefeuille apposent une signature ou un cachet sur au moins une attestation d'unité de portefeuille conforme aux exigences énoncées à l'article 6. Le certificat utilisé pour apposer une signature ou un cachet sur l'attestation d'unité de portefeuille est délivré sur la foi d'un certificat figurant sur la liste de confiance visée dans le règlement d'exécution (UE) 2024/2980.

Article 4

Instances de portefeuille

1. Les instances de portefeuille utilisent au moins un dispositif cryptographique sécurisé de portefeuille pour gérer les actifs critiques.

2. Les fournisseurs de portefeuille garantissent l'intégrité, l'authenticité et la confidentialité de la communication entre les instances de portefeuille et les applications cryptographiques sécurisées de portefeuille.

3. Lorsque des actifs critiques sont liés à l'exécution d'une identification électronique à un niveau de garantie élevé, les opérations cryptographiques de portefeuille ou autres opérations de traitement des actifs critiques sont effectuées conformément aux exigences relatives aux caractéristiques et à la conception des moyens d'identification électronique à un niveau de garantie élevé, telles qu'elles sont énoncées dans le règlement d'exécution (UE) 2015/1502 de la Commission ([11]).

Article 5

Applications cryptographiques sécurisées de portefeuille

1. Les fournisseurs de portefeuille veillent à ce que les applications cryptographiques sécurisées de portefeuille:

a) n'effectuent d'opérations cryptographiques de portefeuille impliquant des actifs critiques autres que celles nécessaires pour que l'unité de portefeuille authentifie l'utilisateur de portefeuille que dans les cas où lesdites applications ont dûment authentifié les utilisateurs de portefeuille;

([11]) 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).

b) lorsqu'elles authentifient des utilisateurs de portefeuille dans le cadre d'une identification électronique à un niveau de garantie élevé, procèdent à l'authentification des utilisateurs de portefeuille conformément aux exigences relatives aux caractéristiques et à la conception des moyens d'identification électronique à un niveau de garantie élevé, telles qu'elles sont énoncées dans le règlement d'exécution (UE) 2015/1502;

c) sont capables de générer de manière sécurisée de nouvelles clés cryptographiques;

d) sont capables de procéder à l'effacement sécurisé d'actifs critiques;

e) sont capables de générer une preuve de la possession de clés privées;

f) protègent les clés privées qu'elles ont générées pendant la durée d'existence des clés;

g) satisfont aux exigences relatives aux caractéristiques et à la conception des moyens d'identification électronique à un niveau de garantie élevé, telles qu'elles sont énoncées dans le règlement d'exécution (UE) 2015/1502;

h) sont les seuls composants capables d'exécuter des opérations cryptographiques de portefeuille et toute autre opération impliquant des actifs critiques dans le cadre d'une identification électronique à un niveau de garantie élevé.

2. Lorsque les fournisseurs de portefeuille décident de fournir une application cryptographique sécurisée de portefeuille à un élément sécurisé intégré, ils fondent leur solution technique sur les spécifications techniques énumérées à l'annexe I ou sur d'autres spécifications techniques équivalentes.

Article 6

Authenticité et validité de l'unité de portefeuille

1. Les fournisseurs de portefeuille veillent à ce que chaque unité de portefeuille contienne des attestations d'unités de portefeuille.

2. Les fournisseurs de portefeuille veillent à ce que les attestations d'unités de portefeuille visées au paragraphe 1 contiennent des clés publiques et que les clés privées correspondantes soient protégées par un dispositif cryptographique sécurisé de portefeuille.

3. Les fournisseurs de portefeuille:

a) informent les utilisateurs de portefeuille de leurs droits et obligations en ce qui concerne leur unité de portefeuille;

b) prévoient des mécanismes, indépendants des unités de portefeuille, pour l'identification et l'authentification sécurisées des utilisateurs de portefeuille;

c) veillent à ce que les utilisateurs de portefeuille aient le droit de demander la révocation de leurs attestations d'unités de portefeuille au moyen des mécanismes d'authentification visés au point b).

Article 7

Révocation des attestations d'unités de portefeuille

1. Les fournisseurs de portefeuille sont les seules entités capables de révoquer les attestations d'unités de portefeuille pour les unités de portefeuille qu'ils ont fournies.

2. Les fournisseurs de portefeuille élaborent et mettent à la disposition du public une politique précisant les conditions et les délais de révocation des attestations d'unités de portefeuille.

3. Lorsque les fournisseurs de portefeuille révoquent des attestations d'unités de portefeuille, ils informent dans les 24 heures les utilisateurs de portefeuille concernés de la révocation de leurs unités de portefeuille, ainsi que de la raison de la révocation et des conséquences qui s'ensuivent pour l'utilisateur du portefeuille. Ces informations sont fournies de manière concise, facilement accessible et dans un langage clair et simple.

4. Lorsque les fournisseurs de portefeuille révoquent des attestations d'unités de portefeuille, ils mettent à la disposition du public le statut de validité de l'attestation d'unité de portefeuille, dans le respect de la vie privée, et décrivent la localisation de ces informations dans l'attestation d'unité de portefeuille.

CHAPITRE III

FONCTIONNALITÉS ET CARACTÉRISTIQUES ESSENTIELLES DES PORTEFEUILLES EUROPÉENS D'IDENTITÉ NUMÉRIQUE

Article 8

Formats des données d'identification personnelle et des attestations électroniques d'attributs

Les fournisseurs de portefeuille veillent à ce que les solutions de portefeuille prennent en charge l'utilisation des données d'identification personnelle et des attestations électroniques d'attributs délivrées conformément à la liste de normes figurant à l'annexe II.

Article 9

Journaux des transactions

1. Que la transaction soit menée à bien ou non, les instances de portefeuille journalisent toutes les transactions avec les parties utilisatrices de portefeuille et les autres unités de portefeuille, y compris les signatures et cachets électroniques.

2. Les informations journalisées comprennent au moins:

a) la date et le lieu de la transaction;

b) le nom, les coordonnées et l'identifiant unique de la partie utilisatrice de portefeuille correspondante ainsi que l'État membre dans lequel cette dernière est établie ou, dans le cas d'autres unités de portefeuille, les informations pertinentes provenant de l'attestation d'unité de portefeuille;

c) le ou les types de données demandées et présentées dans la transaction;

d) dans le cas d'opérations non achevées, la raison de cet inachèvement.

3. Les fournisseurs de portefeuille garantissent l'intégrité, l'authenticité et la confidentialité des informations journalisées.

4. Les instances de portefeuille journalisent les rapports envoyés par l'utilisateur du portefeuille aux autorités chargées de la protection des données par l'intermédiaire de leur unité de portefeuille.

5. Les éléments journalisés visés aux paragraphes 1 et 2 sont accessibles au fournisseur de portefeuille, lorsqu'ils sont nécessaires à la fourniture de services de portefeuille, sur la base du consentement préalable explicite de l'utilisateur de portefeuille.

6. Les éléments journalisés visés aux paragraphes 1 et 2 restent accessibles aussi longtemps que le requiert le droit de l'Union ou le droit national.

7. Les fournisseurs de portefeuille permettent aux utilisateurs de portefeuille d'exporter les informations journalisées visées au paragraphe 2.

Article 10

Divulgation intégrée

1. Les fournisseurs de portefeuille veillent à ce que les attestations électroniques d'attributs dotées de politiques de divulgation intégrées communes au sens de l'annexe III puissent être traitées par les unités de portefeuille qu'ils fournissent.

2. Les instances de portefeuille sont en mesure de traiter et de présenter ces politiques de divulgation intégrées visées au paragraphe 1 en combinaison avec les données reçues de la partie utilisatrice de portefeuille.

3. Les instances de portefeuille vérifient si la partie utilisatrice de portefeuille respecte les exigences de la politique de divulgation intégrée et informent l'utilisateur de portefeuille du résultat.

Article 11

Signatures et cachets électroniques qualifiés

1. Les fournisseurs de portefeuille veillent à ce que les utilisateurs de portefeuille puissent recevoir les certificats qualifiés de signatures ou de cachets électroniques qualifiés qui sont liés à des dispositifs de création de signature ou de cachet qualifiés locaux, extérieurs ou distants par rapport aux instances de portefeuille.

2. Les fournisseurs de portefeuille veillent à ce que les solutions de portefeuille soient capables d'interagir de manière sécurisée avec l'un des types suivants de dispositifs de création de signature ou de cachet qualifiés: dispositifs de création de signature ou de cachet qualifiés locaux, externes ou gérés à distance aux fins de l'utilisation des certificats qualifiés visés au paragraphe 1.

3. Les fournisseurs de portefeuille veillent à ce que les utilisateurs de portefeuille qui sont des personnes physiques disposent, au moins à des fins non professionnelles, d'un accès gratuit aux applications de création de signature permettant la création de signatures électroniques qualifiées gratuites au moyen des certificats visés au paragraphe 1.

Article 12

Applications de création de signature

1. Les applications de création de signature utilisées par les unités de portefeuille peuvent être fournies soit par des fournisseurs de portefeuille, soit par des prestataires de services de confiance, soit par des parties utilisatrices de portefeuille.

2. Les applications de création de signature possèdent les fonctions suivantes:

a) apposer des signatures ou des cachets sur les données fournies par l'utilisateur de portefeuille;

b) apposer des signatures ou des cachets sur les données fournies par la partie utilisatrice;

c) créer des signatures ou des cachets correspondant au moins aux formats obligatoires visés à l'annexe IV;

d) informer les utilisateurs de portefeuille du résultat du processus de création de signature ou de cachet.

3. Les applications de création de signature peuvent être intégrées aux instances de portefeuille ou extérieures à celles-ci. Lorsque les applications de création de signature reposent sur des dispositifs de création de signature qualifiés distants et lorsqu'elles sont intégrées dans des instances de portefeuille, elles prennent en charge l'interface de programmation d'applications visée à l'annexe IV.

Article 13

Exportation des données et portabilité des données

Les unités de portefeuille permettent d'assurer, en fonction des possibilités techniques et hors actifs critiques, l'exportation et la portabilité sécurisées des données à caractère personnel de l'utilisateur du portefeuille, afin de permettre à celui-ci de migrer vers une unité de portefeuille d'une autre solution de portefeuille dans des conditions offrant un niveau de garantie élevé au sens du règlement d'exécution (UE) 2015/1502.

Article 14

Pseudonymes

1. Les unités de portefeuille permettent de générer des pseudonymes pour les utilisateurs de portefeuille conformément aux spécifications techniques énoncées à l'annexe V.

2. Les unités de portefeuille permettent de générer, à la demande d'une partie utilisatrice de portefeuille, un pseudonyme spécifique et exclusif pour cette dernière et lui fournissent ce pseudonyme, soit isolément, soit en combinaison avec toute donnée d'identification personnelle ou attestation électronique d'attributs demandée par elle.

CHAPITRE IV

DISPOSITIONS FINALES

Article 15

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

LISTE DES NORMES VISÉES À L'ARTICLE 5

— SAM.01 «Secured Applications for Mobile — Requirements for supporting 3rd party Applets on eSIM and eSE via SAM» v1.1 2023, GSMA.

— GPC_GUI_ 217 «GlobalPlatform SAM Configuration Technical specification for implementation of SAM» v1.0 2024-04.

— GPC_SPE_0 34 «GlobalPlatform Card Specification Technical specification for smart cards» v2.3.1 2018-03.

— GPC_SPE_0 07 «GlobalPlatform Amendment A Confidential Card Content Management» v1.2 2019-07.

— GPC_SPE_0 13 «GlobalPlatform Amendment D Secure Channel Protocol 03» v1.2 2020-04.

— GPC_SPE_0 93 «GlobalPlatform Amendment F Secure Channel Protocol 11» v1.4 2024-03.

— GPD_SPE_0 75 «Open Mobile API Specification OMAPI API for mobile apps to access secure elements on user devices» v3.3 2018-08, GlobalPlatform.

ANNEXE II

LISTE DES NORMES VISÉES À L'ARTICLE 8

— ISO/IEC.18013-5:2021.

— «Verifiable Credentials Data Model 1.1.», Recommandation W3C, 3 mars 2022.

ANNEXE III

LISTE DES POLITIQUES DE DIVULGATION INTÉGRÉES COMMUNES VISÉES À L'ARTICLE 10

1. «Aucune politique» indique qu'aucune politique ne s'applique aux attestations électroniques d'attributs.
2. «Réservé aux parties utilisatrices autorisées» indique que les utilisateurs de portefeuille ne peuvent divulguer d'attestations électroniques d'attributs qu'aux parties utilisatrices authentifiées qui sont expressément énumérées dans les politiques de divulgation.
3. «Racine de confiance spécifique» indique que les utilisateurs de portefeuille ne devraient divulguer l'attestation électronique d'attributs spécifique qu'aux parties utilisatrices de portefeuille authentifiées qui disposent de certificats d'accès de partie utilisatrice de portefeuille dérivés d'une racine spécifique (ou d'une liste de racines spécifiques) ou d'un ou plusieurs certificats intermédiaires.

ANNEXE IV

FORMATS DES SIGNATURES ET CACHETS VISÉS À L'ARTICLE 12

1. Format de signature ou de cachet obligatoire:

   PAdES (signature électronique avancée au format PDF) comme spécifié dans la norme «ETSI EN 319 142-1 V1.1.1 (2016-04) Signatures électroniques et infrastructures (ESI) — Signatures numériques au format PAdES — Partie 1: blocs de construction et signatures au format de base PAdES».

2. Liste des formats facultatifs de signature ou de cachet:

   a) XAdES comme spécifié dans la norme «ETSI EN 319 132-1 V1.2.1 (2022-02) Signatures électroniques et infrastructures (ESI) — Signatures numériques au format XAdES — Partie 1: blocs de construction et signatures au format de base XAdES» pour la signature au format XML;

   b) JAdES comme spécifié dans la norme «ETSI TS 119 182-1 V1.2.1 (2024-07) Signatures électroniques et infrastructures (ESI) — Signatures numériques au format JAdES — Partie 1: blocs de construction et signatures au format de base JAdES» pour la signature au format JSON;

   c) CAdES (signature électronique avancée au format CMS) comme spécifié dans la norme «ETSI EN 319 122-1 V1.3.1 (2023-06) Signatures électroniques et infrastructures (ESI) — Signatures numériques au format CAdES — Partie 1: blocs de construction et signatures au format de base CAdES» pour la signature au format CMS;

   d) ASiC (conteneur de signatures associées) comme spécifié dans les normes «ETSI EN 319 162-1 V1.1.1 (2016-04) Signatures électroniques et infrastructures (ESI) — Conteneurs de signatures associées (ASiC) — Partie 1: blocs de construction et conteneurs de base ASiC» et «ETSI EN 319 162-2 V1.1.1 (2016-04) Signatures électroniques et infrastructures (ESI) — Conteneurs de signatures associées (ASiC) — Partie 2: conteneurs ASiC complémentaires» pour la signature de conteneurs.

3. Interface de programmation d'application:

   — Cloud Signature Consortium (CSC), spécification v2.0 (20 avril 2023).

ANNEXE V

SPÉCIFICATIONS TECHNIQUES POUR LA CRÉATION DE PSEUDONYMES VISÉE À L'ARTICLE 14

Spécifications techniques:

— WebAuthn — recommandation du W3C, 8 avril 2021, niveau 2, https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.