Journal officiel
de l'Union européenne

FR
Série L

2026/1731

22.7.2026

RÈGLEMENT D'EXÉCUTION (UE) 2026/1731 DE LA COMMISSION

du 15 juillet 2026

modifiant les règlements d'exécution (UE) 2024/2977, (UE) 2024/2979, (UE) 2024/2980 et (UE) 2024/2982 en ce qui concerne les normes et spécifications applicables

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) Afin de garantir le niveau d'harmonisation le plus élevé possible entre les États membres pour le développement des portefeuilles européens d'identité numérique, les spécifications techniques applicables aux portefeuilles s'appuient sur les travaux réalisés sur la base de la recommandation (UE) 2021/946 de la Commission ([2]) et, en particulier, sur l'architecture et le cadre de référence. Étant donné que l'architecture et le cadre de référence ont considérablement évolué depuis les règlements d'exécution (UE) 2024/2977 ([3]), (UE) 2024/2979 ([4]), (UE) 2024/2980 ([5]) et (UE) 2024/2982 ([6]) de la Commission, il convient à présent de modifier ces règlements d'exécution afin de les aligner sur les nouvelles normes, spécifications et procédures.

Conformément aux objectifs du règlement (UE) nº 910/2014, un certain nombre de normes ont été sélectionnées pour satisfaire à ces exigences spécifiques. Ces normes devraient tenir compte des pratiques établies et être largement reconnues dans les secteurs concernés. Par exemple, étant donné que le format VCDM du W3C est utilisé comme format de référence pour les attestations, en particulier dans le secteur de l'éducation, les portefeuilles européens d'identité numérique devraient également prendre en charge ce format lorsque les nouveaux profils au format VCDM du W3C seront disponibles. Si nécessaire, ces normes devraient être adaptées ou complétées afin de garantir la sécurité et la fiabilité des portefeuilles européens d'identité numérique, tout en facilitant l'interopérabilité transfrontière et le bon fonctionnement du marché intérieur.

(2) Pour toute utilisation du portefeuille qui nécessite la présentation du portrait de l'utilisateur de portefeuille, les solutions de portefeuille doivent prendre en charge la fonctionnalité de divulgation sélective et l'utilisateur doit conserver le contrôle total de la divulgation. Afin de préserver la faculté de décider de la divulgation et de protéger le portrait contre une demande de divulgation non intentionnelle ou non autorisée, la conception architecturale des portefeuilles européens d'identité numérique devrait prévoir des mécanismes d'avertissement ainsi que la journalisation de toutes les transactions relatives à l'utilisation du portrait. Pour que l'utilisateur de portefeuille soit conscient qu'il partage des données biométriques, les messages d'avertissement devraient indiquer que la demande

([1]) JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) 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 (JO L 210 du 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reg/2021/946/oj).
([3]) 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).
([4]) 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).
([5]) 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).
([6]) 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).

implique le partage de données biométriques et exiger expressément que la divulgation soit confirmée par l'utilisateur. Lorsqu'une partie utilisatrice traite le portrait aux fins d'identifier une personne physique de manière unique ou de confirmer l'identité déclarée de cette personne, les articles 6 et 9 du règlement (UE) 2016/679 du Parlement européen et du Conseil ([7]) s'appliquent, ainsi que toutes les autres exigences dudit règlement, notamment en ce qui concerne la limitation du traitement du portrait à ce qui est nécessaire à l'utilisation prévue. L'utilisation prévue, ainsi que la demande de divulgation, devraient être communiquées à l'utilisateur de portefeuille dans un langage clair et intelligible. Afin de tenir dûment compte de la sensibilité des données biométriques, il convient que l'utilisateur de portefeuille confirme explicitement et expressément la divulgation. Ni l'absence de réponse ni des cases cochées par défaut ne devraient avoir valeur de confirmation par l'utilisateur de portefeuille. La confirmation explicite de l'utilisateur de portefeuille devrait être une garantie technique et ne devrait pas constituer en soi un fondement juridique pour le traitement. Comme le prévoit l'article 9, paragraphe 4, du règlement (UE) 2016/679, les États membres peuvent maintenir ou instaurer des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement de données génétiques, biométriques, ou de données concernant la santé.

(3) Afin de laisser aux États membres suffisamment de temps pour adapter leurs procédures nationales, le portrait de l'utilisateur de portefeuille peut ne faire partie des données d'identification personnelle obligatoires pour la personne physique qu'à partir du 11 août 2028. Lorsque ces images proviennent de documents d'identité existants, tels que des cartes d'identité ou des passeports, les exigences pertinentes énoncées respectivement dans le règlement (UE) 2025/1208 ([8]) ou le règlement (CE) n° 2252/2004 ([9]) du Conseil s'appliquent.

(4) Le règlement (UE) n° 910/2014 exige que les portefeuilles puissent afficher un label de confiance de l'UE pour le portefeuille d'identité numérique, indiquant de manière vérifiable, simple et reconnaissable qu'un portefeuille a été fourni conformément au règlement. L'utilisation de ce label de confiance contribuera au bon fonctionnement du marché intérieur, garantira une concurrence loyale et protégera les intérêts des consommateurs. Pour permettre l'utilisation de ce label, il convient d'en établir les caractéristiques visuelles et techniques.

(5) Comme le prévoit l'article 12 *ter* du règlement (UE) n° 910/2014, les contrôleurs d'accès doivent permettre aux fournisseurs de portefeuilles européens d'identité numérique et aux émetteurs de moyens d'identification électronique notifiés d'interopérer effectivement avec le même système d'exploitation, les mêmes caractéristiques matérielles et logicielles et, aux fins de l'interopérabilité, d'accéder effectivement à ce même système et à ces mêmes caractéristiques. Cette interopérabilité et cet accès effectifs sont permis gratuitement, et ce, que ces caractéristiques matérielles ou logicielles fassent partie ou non du système d'exploitation, qu'elles soient disponibles ou non pour ce contrôleur d'accès ou qu'elles soient utilisées ou non par ce contrôleur d'accès dans le cadre de la fourniture de tels services. Étant donné que toutes les solutions de portefeuille devraient prendre en charge un ensemble commun de protocoles et d'interfaces afin de garantir la facilité d'utilisation, la sécurité et l'interopérabilité dans tous les États membres, les contrôleurs d'accès devraient activer le système d'exploitation et les caractéristiques matérielles ou logicielles nécessaires à la mise en œuvre des protocoles et interfaces énoncés à l'annexe XII du présent règlement. De ce fait, dans les flux en ligne multi-appareils, tant pour la vérification de proximité physique que pour le transfert de données entre les deux appareils, les contrôleurs d'accès devraient privilégier l'utilisation d'un canal de communication locale tel que prévu par la version 2.3 de la spécification de protocole client-authentificateur (CTAP) ([10]) plutôt que le recours aux services de transport hybride CTAP.

(6) Afin que les États membres, les fournisseurs de certificats d'enregistrement de partie utilisatrice de portefeuille et les fournisseurs de portefeuille disposent de suffisamment de temps pour permettre aux unités de portefeuille d'authentifier et de valider les certificats d'enregistrement de partie utilisatrice de portefeuille, cette exigence ne devrait s'appliquer qu'à partir du 11 août 2028.

(7) Le règlement (UE) 2016/679 et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([11]) s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du présent règlement.

([7]) 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).

([8]) Règlement (UE) 2025/1208 du Conseil du 12 juin 2025 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation (JO L, 2025/1208, 20.6.2025, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres (JO L 385 du 29.12.2004, p. 1, ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) Proposition de norme de l'alliance Fido, Client to Authenticator Protocol (CTAP), 26 février 2026.

([11]) 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).

(8) 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 ([12]) et a rendu son avis le 17 avril 2026 ([13]).

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

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Modification du règlement d'exécution (UE) 2024/2977

Le règlement d'exécution (UE) 2024/2977 est modifié comme suit:

1) L'article 3 *bis* suivant est inséré:

«*Article 3* bis

Protection du portrait

1. Outre les exigences en matière d'informations prévues par le règlement (UE) 2016/679, les fournisseurs de portefeuille veillent à ce que les solutions de portefeuille qu'ils fournissent adressent aux utilisateurs de portefeuille, lorsque les parties utilisatrices de portefeuille demandent la divulgation du portrait, un avertissement indiquant que la demande implique le partage de données biométriques et nécessite l'approbation de la divulgation sélective du portrait.

2. Pour la mise en œuvre de la divulgation sélective du portrait à une partie utilisatrice de portefeuille, les fournisseurs de portefeuille veillent à ce que les solutions de portefeuille demandent à l'utilisateur de portefeuille de confirmer explicitement et expressément la présentation du portrait.

3. Le portrait n'est pas conservé par les parties utilisatrices de portefeuille, à moins que son traitement ne soit nécessaire à des fins d'identification et d'authentification conformément au droit de l'Union en matière de protection des données ou lorsque cela est prévu par le droit de l'Union ou le droit national, conformément au droit de l'Union en matière de protection des données. Il n'est pas transféré à des pays tiers ou à des organisations internationales, à moins que le droit de l'Union en matière de protection des données ne l'autorise.».

2) À l'article 4, le paragraphe 1 est remplacé par le texte suivant:

«1. Les attestations électroniques d'attributs délivrées aux unités de portefeuille sont conformes à au moins une des normes figurant à l'annexe II du règlement d'exécution (UE) 2024/2979.».

3) À l'article 5, paragraphe 4, le point b) est remplacé par le texte suivant:

«b) lorsque l'attestation d'unité de portefeuille de l'unité de portefeuille à laquelle les données d'identification personnelle ont été délivrées a été révoquée;».

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

([12]) 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).

([13]) EDPS Formal comments on the draft Implementing Regulation as regards applicable standards and specifications and correcting Implementing Regulation (EU) 2024/2980 | Contrôleur européen de la protection des données.

Article 2

Modification du règlement d'exécution (UE) 2024/2979

Le règlement d'exécution (UE) 2024/2979 est modifié comme suit:

1) À l'article 3, le paragraphe 2 est supprimé.

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

«a) n'effectuent d'opérations cryptographiques de portefeuille impliquant des actifs critiques stockés dans un dispositif cryptographique sécurisé de portefeuille et non requis pour l'authentification de l'utilisateur de portefeuille que dans les cas où lesdites applications ont authentifié avec succès les utilisateurs de portefeuille;».

3) L'article 5 *bis* suivant est inséré:

«*Article 5* bis

Mécanismes cryptographiques

Aux fins de l'article 4, paragraphe 2, les fournisseurs de portefeuille n'utilisent que les mécanismes cryptographiques visés à l'annexe I *bis*.».

4) L'article 6 est modifié comme suit:

a) le paragraphe 1 est remplacé par le texte suivant:

«1. Les fournisseurs de portefeuille délivrent des attestations d'unité de portefeuille pour chaque unité de portefeuille. Les fournisseurs de portefeuille apposent une signature ou un cachet sur les attestations d'unité de portefeuille de manière à ce que les signatures ou cachets puissent être validés au moyen d'un certificat énuméré conformément à la section 2, point 1), h), de l'annexe II du règlement d'exécution (UE) 2024/2980.»;

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

«2. Les fournisseurs de portefeuille veillent à ce que les attestations d'unité de portefeuille visées au paragraphe 1 soient conformes aux spécifications techniques énoncées à l'annexe I *ter*.»;

c) au paragraphe 3, le point b) est remplacé par le texte suivant:

«b) fournissent aux utilisateurs de portefeuille des mécanismes sécurisés d'identification et d'authentification indépendants des unités de portefeuille;».

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

«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;».

6) À l'article 10, le paragraphe 1 est remplacé par le texte suivant:

«1. Les fournisseurs de portefeuille veillent à ce que les attestations électroniques d'attributs délivrées conformément aux spécifications techniques applicables aux politiques de divulgation intégrées communes au sens de l'annexe III puissent être traitées par les unités de portefeuille qu'ils fournissent.».

7) L'article 12 est modifié comme suit:

a) au paragraphe 2, le point c) est remplacé par le texte suivant:

«c) créer des signatures ou des cachets correspondant au moins au format obligatoire de signature ou de cachet visé à l'annexe IV;»;

b) le paragraphe 3 est remplacé par le texte suivant:

«3. Les applications de création de signature peuvent être intégrées aux instances de portefeuille ou extérieures à celles-ci.»;

c) le paragraphe suivant est inséré:

«4. Les applications de création de signature utilisées par les unités de portefeuille prennent en charge au moins l'interface de programmation d'applications visée à l'annexe IV.».

8) À l'article 14, le paragraphe 1 est supprimé.

9) L'article 14 *bis* suivant est inséré:

«*Article 14* bis

Label de confiance de l'UE pour le portefeuille d'identité numérique

1. Les fournisseurs de portefeuille veillent à ce que les unités de portefeuille affichent le label de confiance de l'UE pour le portefeuille d'identité numérique. Le label de confiance de l'UE pour le portefeuille d'identité numérique se présente sous la forme prévue aux annexes VI et VII.

2. Les fournisseurs de portefeuille font en sorte que les utilisateurs de portefeuille puissent accéder, via les unités de portefeuille, aux informations leur permettant de vérifier l'état de certification de la solution de portefeuille. À cette fin, les fournisseurs de portefeuille veillent à ce que, après l'enregistrement d'une solution de portefeuille, les unités de portefeuille correspondantes comprennent les URL fournies par la Commission européenne pour cette vérification. Les fournisseurs de portefeuille veillent à ce que leurs unités de portefeuille aient accès aux données du label de confiance de l'UE pour le portefeuille d'identité numérique qui sont conformes aux spécifications techniques énoncées à l'annexe VIII.

3. Les couleurs de référence du label de confiance de l'UE pour le portefeuille d'identité numérique sont les couleurs Pantone n° 661 et n° 116; ou, lorsque le procédé par quadrichromie est utilisé, le bleu (100 % cyan + 67 % magenta + 0 % jaune + 40 % noir) et le jaune (0 % cyan + 20 % magenta + 100 % jaune + 0 % noir); lorsque les couleurs RGB sont utilisées, les couleurs de référence sont le bleu (0 rouge + 51 vert + 153 bleu) et le jaune (255 rouge + 204 vert + 0 bleu).

4. La version en noir et blanc du label de confiance de l'UE pour le portefeuille d'identité numérique figurant à l'annexe VII peut être utilisée uniquement dans les cas où l'utilisation de la couleur n'est pas possible pour des raisons pratiques.

5. Lorsque le label de confiance de l'UE pour le portefeuille d'identité numérique est placé sur fond foncé, il peut être utilisé en négatif, en reprenant la même couleur de fond. Lorsque la version en couleurs du label de confiance de l'UE pour le portefeuille d'identité numérique est utilisée sur un fond coloré qui rend le label difficile à voir, une ligne de délimitation extérieure peut être tracée autour du label afin de renforcer le contraste avec le fond.

6. Le label de confiance de l'UE pour le portefeuille d'identité numérique a une taille minimale de 64 × 85 pixels à 150 dpi.

7. Les fournisseurs de portefeuille font en sorte que l'utilisation du label de confiance de l'UE pour le portefeuille d'identité numérique permette de déterminer clairement à quelle unité de portefeuille ce label se rapporte. Le label de confiance de l'UE pour le portefeuille d'identité numérique peut être associé à des éléments graphiques ou textuels indiquant clairement pour quelle unité de portefeuille il est utilisé, à condition qu'ils n'affectent ni sa capacité à être reconnu comme label de confiance de l'UE pour le portefeuille d'identité numérique, ni l'association à la liste des portefeuilles européens d'identité numérique certifiés visée à l'article 5 *quinquies* du règlement (UE) n° 910/2014.

8. Lorsque les fournisseurs de portefeuille ont révoqué une attestation d'unité de portefeuille, ils veillent à ce que le label de confiance de l'UE pour le portefeuille d'identité numérique ne soit plus affiché par l'unité de portefeuille correspondante.».

10) Les annexes I *bis* et I *ter* sont ajoutées, telles qu'elles figurent à l'annexe II et à l'annexe III du présent règlement.

11) L'annexe II est remplacée par l'annexe IV du présent règlement.

12) L'annexe III est remplacée par l'annexe V du présent règlement.

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

14) L'annexe V est supprimée.

15) Le texte figurant à l'annexe VII du présent règlement est inséré comme annexe VI.

16) Le texte figurant à l'annexe VIII du présent règlement est inséré comme annexe VII.

17) Le texte figurant à l'annexe IX du présent règlement est inséré comme annexe VIII.

Article 3

Modifications du règlement d'exécution (UE) 2024/2980

Le règlement d'exécution (UE) 2024/2980 est modifié comme suit:

1. À l'article 5, le paragraphe 2 est remplacé par le texte suivant:

«2. Le cas échéant, la Commission établit, tient à jour et publie une liste reprenant les informations notifiées par les États membres concernant les fournisseurs de portefeuille, les fournisseurs de données d'identification personnelle, les fournisseurs de certificats d'accès de partie utilisatrice de portefeuille et les fournisseurs de certificats d'enregistrement de partie utilisatrice de portefeuille, telles qu'elles sont énumérées à l'annexe II, sections 2, 3, 4 et 5.».

2. L'annexe II du règlement d'exécution (UE) 2024/2980 est modifiée conformément à l'annexe X du présent règlement.

Article 4

Modifications du règlement d'exécution (UE) 2024/2982

Le règlement d'exécution (UE) 2024/2982 est modifié comme suit:

1) À l'article 1er, le paragraphe 2 est remplacé par le texte suivant:

«2) la présentation des attributs des données d'identification personnelle et des attestations électroniques d'attributs aux parties utilisatrices de portefeuille;».

2) L'article 3 est modifié comme suit:

a) le point 1) est remplacé par le texte suivant:

«1) authentifient et valident les certificats d'accès de partie utilisatrice de portefeuille lors d'interactions avec des parties utilisatrices de portefeuille sans déléguer l'exécution de ces processus à un navigateur du système d'exploitation ou à une autre application intermédiaire;»;

b) le point 2) est supprimé;

c) le point 3) est remplacé par le texte suivant:

«3) authentifient et valident les demandes introduites au moyen de certificats d'accès de partie utilisatrice de portefeuille;»;

d) le point 4) est remplacé par le texte suivant:

«4) authentifient et valident le certificat d'enregistrement de partie utilisatrice de portefeuille;»;

e) le point 5) est remplacé par le texte suivant:

«5) affichent aux utilisateurs de portefeuille les informations contenues dans les certificats d'accès de partie utilisatrice de portefeuille;»;

f) le point 8) est supprimé;

g) le point 9) est remplacé par le texte suivant:

«9) ne présentent aucun attribut demandé aux parties utilisatrices de portefeuille tant que les conditions suivantes ne sont pas remplies:

a) il a été vérifié que les politiques de divulgation intégrées ont été traitées au sein de l'unité de portefeuille conformément à l'article 10 du règlement d'exécution (UE) 2024/2979;

b) il a été vérifié que les utilisateurs de portefeuille ont approuvé partiellement ou intégralement la présentation;».

3) À l'article 4, le paragraphe 1 est remplacé par le texte suivant:

«1. Les fournisseurs de portefeuille veillent à ce que les solutions de portefeuille prennent en charge les protocoles et les interfaces figurant à l'annexe I pour la délivrance de données d'identification personnelle et d'attestations électroniques d'attributs aux unités de portefeuille.».

4) L'article 5 est modifié comme suit:

a) les paragraphes 1 et 2 sont remplacés par le texte suivant:

«1. Les fournisseurs de portefeuille veillent à ce que les solutions de portefeuille prennent en charge les protocoles et les interfaces permettant la présentation d'attributs aux parties utilisatrices de portefeuille, à distance et, le cas échéant, à proximité, conformément aux spécifications techniques figurant à l'annexe II.

2. Les fournisseurs de portefeuille veillent à ce que, à la demande des utilisateurs, les unités de portefeuille répondent aux demandes dûment authentifiées et validées des parties utilisatrices de portefeuille mentionnées à l'article 3, conformément aux spécifications techniques figurant à l'annexe II.»;

b) le paragraphe 5 est supprimé.

5) L'article 8 est remplacé par le texte suivant:

«*Article 8*

Entrée en vigueur

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

L'article 3, paragraphe 4, s'applique à compter du 11 août 2028.

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

6) L'annexe est supprimée.

7) Le texte figurant à l'annexe XI du présent règlement est ajouté en tant qu'annexe I.

8) Le texte figurant à l'annexe XII du présent règlement est ajouté en tant qu'annexe II.

Article 5

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 15 juillet 2026.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE I

«ANNEXE

Spécifications techniques relatives aux données d'identification personnelle visées à l'article 3, paragraphe 3

Section 1: Ensemble de données d'identification des personnes physiques

Tableau 1

Données d'identification personnelle obligatoires pour les personnes physiques soumises à la divulgation sélective

Identifiant de données	Définition
`family_name`	Nom(s) de famille actuel(s) de l'utilisateur auquel se rapportent les données d'identification personnelle.
`given_name`	Prénom(s) actuel(s), y compris, le cas échéant, le(s) deuxième(s) prénom(s), de l'utilisateur auquel se rapportent les données d'identification personnelle.
`birth_date`	Jour, mois et année de naissance de l'utilisateur auquel se rapportent les données d'identification personnelle.
`birth_place`	Le code pays alpha-2, tel que spécifié dans la norme ISO 3166-1, ou la subdivision de l'État, la province, le district, le territoire ou la municipalité, la ville ou le village où est né l'utilisateur auquel les données d'identification personnelle se rapportent.
`nationality`	Un ou plusieurs codes pays alpha-2 spécifiés dans la norme ISO 3166-1, représentant la nationalité de l'utilisateur auquel se rapportent les données d'identification personnelle.
`portrait`	Sauf refus exprès de l'utilisateur, le cas échéant, l'image faciale de l'utilisateur auquel se rapportent les données d'identification personnelle, conforme aux exigences de qualité applicables à un type d'image frontale complète du visage énoncées dans la norme ISO/IEC 39794-5 ou, aux fins de la compatibilité rétrospective, dans la norme ISO/IEC 19794-5, paragraphes 8.2, 8.3 et 8.4, fournie sous forme de données d'image encodées sans les en-têtes ou les blocs comme spécifié dans le paragraphe 5 de la norme ISO/IEC 19794-5, à l'exception des données d'image proprement dites (un JPEG), est applicable à partir du 11 août 2028.

— Les États membres peuvent prévoir que l'utilisateur a la faculté de refuser l'insertion du portrait dans les données d'identification personnelle.

— Les États membres doivent veiller à ce que la divulgation sélective s'applique à chaque identifiant de données, y compris le portrait.

— Si la date de naissance de la personne physique n'est pas connue, les États membres doivent choisir des valeurs appropriées conformes aux spécifications mentionnées aux sections 4.1 ou 4.2 (selon le cas) de la présente annexe.

— Si la nationalité de la personne physique est inconnue, les États membres doivent utiliser la valeur 'QU'.

— Si la personne physique ne possède pas de nationalité, les États membres doivent utiliser la valeur 'QS'.

— Si l'utilisateur refuse l'insertion du portrait, les États membres doivent laisser la valeur vide.

Tableau 2

Données d'identification personnelle facultatives pour les personnes physiques soumises à la divulgation sélective

Identifiant de données	Définition
resident_address	L'adresse complète du lieu où l'utilisateur auquel se rapportent les données d'identification personnelle réside actuellement ou peut être contacté (nom de rue, numéro de maison, ville, etc.).
resident_country	Le pays où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle, sous la forme d'un code pays alpha-2, tel que spécifié dans la norme ISO 3166-1.
resident_state	La subdivision de l'État, la province, le district ou le territoire où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle.
resident_city	La municipalité, la ville ou le village où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle.
resident_postal_code	Le code postal du lieu où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle.
resident_street	Le nom de la rue où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle, y compris le numéro de la maison et tout affixe ou suffixe de ce numéro.
personal_administrative_-number	Une valeur attribuée à l'utilisateur auquel se rapportent les données d'identification personnelle, qui est unique parmi tous les numéros administratifs personnels délivrés par le fournisseur de données d'identification personnelle. Lorsque les États membres choisissent d'inclure cet attribut, ils doivent décrire dans leurs schémas d'identification électronique en vertu desquels les données d'identification personnelle sont délivrées la politique qu'ils appliquent aux valeurs de cet attribut, y compris, le cas échéant, les conditions spécifiques applicables au traitement de cette valeur.
family_name_birth	Nom(s) de famille de l'utilisateur auquel se rapportent les données d'identification personnelle au moment de la naissance.
given_name_birth	Prénom(s), y compris le(s) deuxième(s) prénom(s), de l'utilisateur auquel se rapportent les données d'identification personnelle au moment de la naissance.
sex	La valeur est l'une des suivantes: 0 = inconnu; 1 = masculin; 2 = féminin; 3 = autre; 4 = inter; 5 = divers; 6 = ouvert; 9 = sans objet. Pour les valeurs 0, 1, 2 et 9, la norme ISO/IEC 5218 s'applique.
email_address	Adresse de courrier électronique de l'utilisateur auquel se rapportent les données d'identification personnelle [conformément à la norme RFC 5322 [1]].

Identifiant de données	Définition
`mobile_phone_number`	Numéro de téléphone portable de l'utilisateur auquel se rapportent les données d'identification personnelle, commençant par le symbole "+", comme préfixe d'appel international, et l'indicatif téléphonique international, suivis de numéros uniquement.

([1]) P. Resnick, éd., "Format de message Internet", RFC 5322, octobre 2008.

Section 2: Ensemble de donnés d'identification des personnes morales

Tableau 3

Données d'identification personnelle obligatoires pour les personnes morales

Identifiant de données
Dénomination sociale actuelle
Un identifiant unique créé par l'État membre expéditeur conformément aux spécifications techniques aux fins de l'identification transfrontière et qui soit aussi persistant que possible dans le temps

— Lorsqu'un identifiant de données n'est pas connu pour la personne ou ne peut pas être délivré autrement dans le cadre de l'ensemble de données d'identification personnelle, les États membres doivent utiliser à la place une valeur d'attribut adaptée à la situation.

Tableau 4

Données d'identification personnelle facultatives pour les personnes morales

Identifiant de données
Adresse actuelle
Numéro d'identification TVA
Numéro de référence fiscal
Identifiant unique européen visé dans la directive (UE) 2017/1132 du Parlement européen et du Conseil ([1])
Identifiant d'entité juridique (LEI) visé dans le règlement d'exécution (UE) 2022/1860 de la Commission ([2])
Numéro d'enregistrement et d'identification des opérateurs économiques (numéro EORI) visé dans le règlement d'exécution (UE) n° 1352/2013 de la Commission ([3])
Numéro d'accise visé à l'article 2, point 12), du règlement (UE) n° 389/2012 du Conseil ([4])

([1]) Directive (UE) 2017/1132 du Parlement européen et du Conseil du 14 juin 2017 relative à certains aspects du droit des sociétés (JO L 169 du 30.6.2017, p. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) Règlement d'exécution (UE) 2022/1860 de la Commission du 10 juin 2022 définissant des normes techniques d'exécution pour l'application du règlement (UE) n° 648/2012 du Parlement européen et du Conseil en ce qui concerne les normes, les formats, la fréquence et les méthodes et modalités de déclaration (JO L 262 du 7.10.2022, p. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Règlement d'exécution (UE) n° 1352/2013 de la Commission du 4 décembre 2013 établissant les formulaires prévus par le règlement (UE) n° 608/2013 du Parlement européen et du Conseil concernant le contrôle, par les autorités douanières, du respect des droits de propriété intellectuelle (JO L 341 du 18.12.2013, p. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) Règlement (UE) n° 389/2012 du Conseil du 2 mai 2012 concernant la coopération administrative dans le domaine des droits d'accise et abrogeant le règlement (CE) n° 2073/2004 (JO L 121 du 8.5.2012, p. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

3. Section 3: Ensemble de métadonnées relatives aux données d'identification des personnes

Tableau 5

Métadonnées relatives aux données d'identification des personnes

Identifiant de données	Définition	Présence
`issuing_authority`	Nom de l'autorité administrative qui a délivré les données d'identification personnelle, ou code pays ISO 3166 alpha-2 de l'État membre concerné s'il n'existe pas d'autorité distincte habilitée à délivrer les données d'identification personnelle.	Obligatoire
`issuing_country`	Code pays alpha-2, tel que spécifié dans la norme ISO 3166-1, du pays ou territoire du fournisseur des données d'identification personnelle.	Obligatoire
`expiry_date`	Date (et, si possible, heure) à laquelle la période de validité administrative des données d'identification personnelle expire.	Facultatif
`document_number`	Un numéro pour les données d'identification personnelle, attribué par le fournisseur de données d'identification personnelle.	Facultatif
`issuing_jurisdiction`	Code de subdivision du pays correspondant à l'entité territoriale qui a émis les données d'identification personnelle, conformément au paragraphe 8 de la norme ISO 3166-2:2020. La première partie du code est identique à la valeur correspondant au pays de délivrance.	Facultatif
`issuance_date`	Date et, si possible, heure auxquelles la période de validité administrative des données d'identification personnelle a commencé.	Facultatif

4) Section 4: Encodage des attributs de données d'identification des personnes physiques

— Les données d'identification des personnes physiques doivent être délivrées conformément aux normes mentionnées à l'annexe II du règlement d'exécution (UE) 2024/2979, paragraphes 5 (format SD-JWT VC) et 6 (format ISO/IEC-mdoc), applicables aux attestations électroniques d'attributs. Les paragraphes 5.2.2, 5.2.4, 5.2.5, EAA-6.1-03, 6.2.2, 6.2.3, 6.2.4 et 6.2.5 ne s'appliquent pas.

— L'encodage des données d'identification des personnes physiques doit être conforme aux spécifications techniques énoncées aux sections 4.1 et 4.2 de la présente annexe.

4.1 Encodage des données d'identification des personnes physiques au format ISO/IEC-mdoc

— Le type d'attestation pour les données d'identification personnelle au format ISO/IEC-mdoc doit être 'eu.europa.ec.eudi.pid.1'. L'identifiant de l'espace de noms pour les attributs de données d'identification personnelle figurant dans la présente annexe doit être 'eu.europa.ec.eudi.pid.1'.

— Si les données d'identification personnelle comprennent des données pour lesquelles la présente annexe ne prévoit pas d'identifiants de données, ces données doivent être définies dans un espace de noms (infra)national alloué aux données d'identification personnelle qui utilise le format général eu.europa.ec.eudi.pid.[code pays ISO 3166-1 alpha-2 ou code région ISO 3166-2] suivi d'un point et d'un numéro de version facultatifs.

— Si l'espace de noms (infra)national est utilisé, son programme, comprenant tous les identifiants de données, leur définition, leur présence et leur format d'encodage, doit être publié conformément à l'article 8 du règlement d'exécution (UE) 2025/1569 de la Commission ([1]).

— Les données d'identification personnelle et leurs métadonnées mentionnées aux sections 1 et 3 de la présente annexe doivent figurer dans les éléments de données d'identification personnelle au sens des spécifications du format ISO/IEC-mdoc.

— Le membre deviceKey au sein du membre deviceKeyInfo de l'instance du type MobileSecurityObject contient une clé publique.

— Cette clé publique doit correspondre à une clé privée qui est stockée dans le dispositif cryptographique sécurisé de portefeuille ("wallet secure cryptographic device", ou "WSCD") de l'utilisateur de portefeuille.

— L'en-tête protégé de la signature numérique CB-AdES qui signe une donnée d'identification personnelle au format ISO/IEC-mdoc doit contenir les paramètres d'en-tête x5u et x5t, tous deux spécifiés dans la RFC 9360 ([2]).

— L'algorithme de hachage utilisé dans le paramètre d'en-tête x5t doit être SHA-256.

— Les exigences applicables à l'encodage des données d'identification personnelle au format ISO/IEC-mdoc figurent dans le tableau 6.

Tableau 6

Exigences applicables à l'encodage des données d'identification personnelle au format ISO/IEC-mdoc

Identifiant de données	Identifiant d'attribut	Format d'encodage
family_name	family_name	tstr
given_name	given_name	tstr
birth_date	birth_date	full-date
birth_place	place_of_birth	place_of_birth
nationality	nationality	nationalities
resident_address	resident_address	tstr
resident_country	resident_country	tstr
resident_state	resident_state	tstr
resident_city	resident_city	tstr
resident_postal_code	resident_postal_code	tstr
resident_street	resident_street	tstr
personal_administrative_number	personal_administrative_number	tstr
portrait	portrait	bstr
family_name_birth	family_name_birth	tstr
given_name_birth	given_name_birth	tstr
sex	sex	uint

([1]) Règlement d'exécution (UE) 2025/1569 de la Commission du 29 juillet 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les attestations électroniques d'attributs qualifiées et les attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte (JO L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([2]) J. Schaad, "Signature et chiffrement d'objet CBOR (COSE): paramètres d'en-tête pour porter et référencer les certificats X.509" (https://datatracker.ietf.org/doc/rfc9360/).

Identifiant de données	Identifiant d'attribut	Format d'encodage
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate ou full-date
issuing_authority	issuing_authority	tstr
issuing_country	issuing_country	tstr
document_number	document_number	tstr
issuing_jurisdiction	issuing_jurisdiction	tstr
issuance_date	issuance_date	tdate ou full-date

— La notation du format d'encodage des attributs spécifiés dans le tableau 6 utilise les types de représentation spécifiés dans la RFC 8610 ([3]), moyennant les exigences supplémentaires suivantes:

a) les tstr doivent être encodées en UTF-8;

b) les tstr doivent prendre en charge toute la plage Unicode;

c) les tstr doivent avoir une longueur maximale de 150 caractères;

d) les dates doivent être encodées conformément à la RFC 8943 ([4]);

e) l'attribut full-date doit être interprété comme #6.1004(tstr), le tag 1004 étant spécifié dans la RFC 8943;

f) l'attribut tdate doit contenir une chaîne date-heure telle que spécifiée dans la RFC 3339 ([5]);

g) l'attribut full-date doit contenir une chaîne full-date telle que spécifiée dans la RFC 3339, conformément à la RFC 8943;

h) sauf indication contraire, la représentation d'une date dans les attributs:

— ne doit pas utiliser de fractions de seconde;

— ne doit pas utiliser de décalage de temps local par rapport à l'UTC et le décalage de temps spécifié dans la RFC 3339 doit être fixé à 'Z';

i) les nombres entiers ayant les types majeurs 0 et 1 doivent être aussi petits que possible, comme spécifié dans la RFC 8949, section 4.2 ([6]);

j) l'attribut place_of_birth doit contenir au moins une des paires clé-valeur suivantes: 'country', 'region' ou 'locality';

k) l'expression de la longueur dans une bstr, une tstr, un tableau ou une table associative doit être aussi courte que possible, comme spécifié dans la RFC 8949, section 4.2;

([3]) C. Vigano et H. Birkholz, "Langage de définition concise de données (CDDL): convention de notation pour exprimer la représentation concise d'objet binaire CBOR) et les structures de données Jason", RFC 8610, juin 2019.
([4]) M. Jones, A. Nadalin et J. Richter, "Étiquettes de représentation concise d'objet binaire (CBOR) pour la date", RFC 8943, novembre 2020.
([5]) G. Klyne et C. Newman, "La date et l'heure sur l'Internet: horodatages", RFC 3339, juillet 2002.
([6]) C. Bormann et P. Hoffman, "Représentation concise d'objet binaire (CBOR)", RFC 8949, décembre 2020.

l) l'attribut nationality doit être encodé sous la forme d'un tableau de codes pays alpha-2, conformément à la norme ISO 3166-1. Lorsque la notation CDDL telle que spécifiée dans le RFC 8610 est utilisée, l'encodage de cet attribut doit être le suivant:

— nationalities = [+ CountryCode];

— CountryCode = tstr; code pays alpha-2 spécifié dans la norme ISO 3166-1;

— lorsqu'un utilisateur de portefeuille auquel se rapportent les données d'identification personnelle possède plusieurs nationalités et que le fournisseur de données d'identification personnelle atteste ces nationalités multiples, le fournisseur de données d'identification personnelle peut inclure toutes les nationalités dans les données d'identification personnelle;

— l'attribut place_of_birth doit être encodé comme un type place_of_birth. Lorsque la notation CDDL telle que spécifiée dans le RFC 8610 est utilisée, l'encodage de cet attribut doit être le suivant:

place_of_birth =

{

? 'country': tstr; un code pays alpha-2 unique comme spécifié dans la norme ISO 3166-1

? 'region': tstr; le nom de la subdivision de l'État, de la province, du district ou du territoire

? 'locality': tstr; le nom de la municipalité, de la ville ou du village

}

4.2 Exigences applicables à l'encodage des données d'identification personnelle au format SD-JWT VC

— Les données d'identification personnelle et leurs métadonnées mentionnées dans la présente section doivent figurer dans les données d'identification personnelle en tant que revendications au sens des spécifications du format SD-JWT VC.

— Toutes les revendications figurant dans les données d'identification personnelle délivrées, mentionnées au tiret précédent, doivent pouvoir faire l'objet d'une divulgation sélective de manière individuelle, à l'exception des revendications définies comme ne pouvant pas faire l'objet d'une divulgation sélective dans le format SD-JWT VC.

— Le tableau 7 détermine l'encodage des noms de revendications qui sont des noms publics.

— Le tableau 8 détermine l'encodage des noms de revendications qui sont propres aux données d'identification personnelle.

— Les chaînes JSON utilisées dans des données d'identification personnelle encodées au format SD-JWT VC doivent être encodées en UTF-8 et prendre en charge toute la plage Unicode, sauf indication contraire expresse dans le tableau 8 ci-dessous ou dans les références qui y figurent.

— Les revendications JWT nbf et exp, telles que définies dans la RFC 7519 ([7]), doivent être utilisées pour exprimer la période de validité technique des données d'identification personnelle en conformité avec le format SD-JWT VC.

([7]) J. Jones et autres, "Jeton JSON sur la Toile (JWT)", RFC 7519, mai 2015.

— Les données d'identification personnelle doivent comprendre la revendication cnf telle que définie dans la RFC 7800 ([8]), qui doit être une clé publique générée à partir d'une clé privée stockée dans le WSCD de l'unité de portefeuille de l'utilisateur de portefeuille.

— L'en-tête protégé de la signature numérique qui signe une donnée d'identification personnelle au format SD-JWT VC contient les paramètres d'en-tête x5u et x5t#S256, spécifiés dans la RFC 7515 ([9]).

Tableau 7

Exigences applicables à l'encodage des données d'identification personnelle au format SD-JWT VC utilisant des noms publics

Identifiant de données	Identifiant d'attribut	Format d'encodage
`family_name`	`family_name`	chaîne de caractères
`given_name`	`given_name`	chaîne de caractères
`birth_date`	`birthdate`	chaîne de caractères, ISO 8601-1, format AAAA-MM-JJ
`birth_place`	`place_of_birth`	structure JSON
`nationality`	`nationalities`	tableau de chaînes
`resident_address`	`address.formatted`	chaîne de caractères
`resident_country`	`address.country`	chaîne de caractères
`resident_state`	`address.region`	chaîne de caractères
`resident_city`	`address.locality`	chaîne de caractères
`resident_postal_code`	`address.postal_code`	chaîne de caractères
`resident_street`	`address.street_address`	chaîne de caractères
`family_name_birth`	`birth_family_name`	chaîne de caractères
`given_name_birth`	`birth_given_name`	chaîne de caractères
`email_address`	`email`	chaîne de caractères
`mobile_phone_number`	`phone_number`	chaîne de caractères
`portrait`	`picture`	chaîne de caractères; URL de données contenant un portrait encodé en base 64 au format JPEG

([8]) M. Jones et autres, "Sémantique de clé de preuve de possession pour jetons JSON de la Toile", RFC 7800, avril 2016.
([9]) M. Jones et autres, "Signature JSON sur la Toile (JWS)", RFC 7515, mai 2015.

Tableau 8

Exigences applicables à l'encodage des données d'identification personnelle au format SD-JWT VC utilisant des noms privés

Identifiant de données	Identifiant d'attribut	Format d'encodage
`expiry_date`	`date_of_expiry`	chaîne de caractères, ISO 8601-1, format AAAA-MM-JJ
`issuance_date`	`date_of_issuance`	chaîne de caractères, ISO 8601-1, format AAAA-MM-JJ
`personal_administrative_number`	`personal_administrative_number`	chaîne de caractères
`sex`	`sex`	valeur numérique
`issuing_authority`	`issuing_authority`	chaîne de caractères
`issuing_country`	`issuing_country`	chaîne de caractères
`document_number`	`document_number`	chaîne de caractères
`issuing_jurisdiction`	`issuing_jurisdiction`	chaîne de caractères

— Le type de base des données d'identification personnelle doit être 'urn:eudi:pid:1', inclus dans la revendication vct. Toutes les données d'identification personnelle doivent utiliser des types compris dans l'espace de noms 'urn:eudi:pid:'.

— Si les données d'identification personnelle comprennent des attributs qui ne sont pas spécifiés dans la présente annexe, ces attributs sont définis au sein d'un type (infra)national.

— Si le type (infra)national est utilisé, son programme, comprenant tous les identifiants de données, leur définition, leur présence et leur format d'encodage, doit être défini dans un programme publié conformément à l'article 8 du règlement d'exécution (UE) 2025/1569.

Section 5: Détails de l'infrastructure de confiance

La liste des fournisseurs de données d'identification personnelle mise à disposition par la Commission conformément au règlement d'exécution (UE) 2024/2980 permet d'authentifier les données d'identification personnelle.».

ANNEXE II

«*ANNEXE I bis*

Mécanismes cryptographiques visés à l'article 5 *bis*

Groupe européen de certification de cybersécurité, sous-groupe sur la cryptographie: "Agreed Cryptographic Mechanisms", publié par l'Agence de l'Union européenne pour la cybersécurité (ENISA) ([1]).».

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

ANNEXE III

«ANNEXE I ter

Spécifications techniques pour les attestations d'unité de portefeuille visées à l'article 6, paragraphe 2 *bis*

1) Une attestation d'unité de portefeuille doit comprendre une ou plusieurs attestations d'instance de portefeuille et une ou plusieurs attestations de clé.

2) L'attestation d'instance de portefeuille et les attestations de clé doivent satisfaire aux exigences suivantes:

a) Exigences en matière de format

— FR-WIA-1: une attestation d'instance de portefeuille doit être un jeton Web JSON (JWT) tel que défini dans la RFC 7519 ([1]), sur lequel le fournisseur de portefeuille a apposé sa signature ou son cachet au moyen d'une signature JAdES compacte conforme au niveau de base B.

— FR-WIA-1.1: une attestation d'instance de portefeuille doit être une attestation de portefeuille telle que définie à l'appendice E de la spécification "OpenID for Verifiable Credential Issuance v1.0" ([2]) ('OID4VCI ') et étendue comme indiqué dans les paragraphes C-WIA-1 et C-WIA-2 ci-dessous.

— FR-KA-1: une attestation de clé doit être un JWT tel que défini dans la RFC 7519, sur lequel le fournisseur de portefeuille a apposé sa signature ou son cachet au moyen d'une signature JAdES compacte conforme au niveau de base B.

— FR_KA_1.1: une attestation de clé doit être une attestation de clé telle que définie à l'appendice D de la spécification OID4VCI, étendue comme indiqué dans les paragraphes C_KA-1 et C_KA-2 ci-dessous.

b) Exigences en matière de transport

— TR-WIA-1: une unité de portefeuille doit utiliser une attestation d'instance de portefeuille lors de la délivrance de données d'identification personnelle, d'attestations électroniques d'attributs qualifiées ou non qualifiées ou d'attestations électroniques d'attributs fournies par un organisme du secteur public responsable d'une source authentique ou pour son compte.

— TR-WIA-2: un fournisseur de portefeuille doit vérifier l'intégrité de l'instance de portefeuille et apposer sa signature ou son cachet sur l'attestation d'instance de portefeuille.

— TR-WIA-2.1: lorsqu'un fournisseur de portefeuille délivre une attestation d'instance de portefeuille, la différence entre l'heure à laquelle le fournisseur de portefeuille a vérifié l'intégrité de l'instance de portefeuille et l'heure qu'il indiquera dans le paramètre d'en-tête 'exp' de l'attestation d'instance de portefeuille délivrée doit être inférieure à 24 heures.

— TR-WIA-2.2: le fournisseur de portefeuille doit veiller à ce qu'une unité de portefeuille contienne les attestations d'instance de portefeuille nécessaires à la délivrance des données d'identification personnelle et des attestations électroniques d'attributs.

— TR-WIA-3: lors de la délivrance, une unité de portefeuille doit envoyer une attestation d'instance de portefeuille au serveur d'autorisation dans la demande d'autorisation poussée et la demande de jeton, comme indiqué dans la spécification OID4VCI.

— TR-WIA-3.1: une unité de portefeuille doit envoyer l'attestation d'instance de portefeuille accompagnée d'une preuve de possession ('PoP'), comme indiqué à l'appendice E de la spécification OID4VCI.

— TR-WIA-3.2: une unité de portefeuille ne doit envoyer la même attestation d'instance de portefeuille qu'à un seul serveur d'autorisation.

([1]) RFC 7519: Jeton JSON sur la Toile (JWT), mai 2015.
([2]) "OpenID for Verifiable Credential Issuance v1.0", https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

— TR-WIA-3.2.1: lorsqu'un fournisseur de portefeuille utilise l'option 'per-issuer reuse' spécifiée dans le paragraphe R_WIA_1 ci-dessous, une unité de portefeuille peut envoyer plusieurs fois une attestation d'instance de portefeuille au même serveur d'autorisation.

— TR-WIA-3.2.2: lorsqu'un fournisseur de portefeuille n'utilise pas l'option 'per-issuer reuse', une unité de portefeuille doit utiliser une attestation d'instance de portefeuille dans un seul processus de délivrance au maximum.

— TR-WIA-4: lorsqu'un serveur d'autorisation reçoit une attestation d'instance de portefeuille, il doit vérifier la signature de l'attestation d'instance de portefeuille en utilisant la clé publique contenue dans le certificat de signature inclus dans le paramètre 'x5c' de l'en-tête JOSE de l'attestation d'instance de portefeuille.

— TR-WIA-4.1: le serveur d'autorisation doit vérifier également que ce certificat de signature peut être vérifié avec une ancre de confiance sur la liste des fournisseurs de portefeuille visée à l'article 5 du règlement d'exécution (UE) 2024/2980, en utilisant éventuellement des certificats intermédiaires inclus dans le paramètre x5c.

— TR-WIA-4.2: le serveur d'autorisation doit vérifier que l'attestation d'instance de portefeuille n'a pas expiré.

— TR-WIA-4.3: le serveur d'autorisation doit vérifier la signature de la PoP en utilisant la clé publique figurant dans la revendication 'cnf'.

— TR_KA-1: une unité de portefeuille doit utiliser une attestation de clé lors de la délivrance de données d'identification personnelle et lors de la délivrance d'attestations électroniques d'attributs qualifiées ou non qualifiées liées à un appareil ou d'attestations électroniques d'attributs fournies par un organisme du secteur public responsable d'une source authentique ou pour son compte.

— TR_KA-1.1: une unité de portefeuille ne doit pas utiliser d'attestation de clé lors de la délivrance d'attestations électroniques d'attributs qualifiées ou non qualifiées liées à un appareil ou d'attestations électroniques d'attributs fournies par un organisme du secteur public responsable d'une source authentique ou pour son compte.

— TR_KA-2: un fournisseur de portefeuille doit fournir à une unité de portefeuille des attestations de clé différentes pour le WSCD de l'unité de portefeuille et pour chacun de ses magasins de clés.

— TR_KA-2.1: le fournisseur de portefeuille doit apposer sa signature ou son cachet sur une attestation de clé après avoir vérifié que les clés attestées dans l'attestation de clé sont stockées dans le WSCD de l'unité de portefeuille ou le magasin de clés décrit dans l'attestation de clé.

— TR_KA-2.2: une attestation de clé doit contenir au moins une clé publique attestée. Le nombre de clés contenues dans l'attestation de clé envoyée à un émetteur de justificatifs d'identité ne devrait pas dépasser la taille de lot maximale définie par ledit émetteur dans ses métadonnées; voir ETSI TS 119 472-3 ([3]), paramètre 'credential_configurations_supported. credential_metadata.credential_reuse_policy.options.batch_size'.

— TR_KA-2.3: un fournisseur de portefeuille doit inclure une clé publique (correspondant à une clé privée stockée dans le WSCD ou le magasin de clés de l'unité de portefeuille) dans une seule attestation de clé au maximum.

— TR_KA-2.4: une unité de portefeuille doit utiliser une attestation de clé lors d'un seul processus de délivrance ou de redélivrance de justificatif d'identité au maximum.

— TR_KA-2.5: un fournisseur de portefeuille doit veiller à ce qu'une unité de portefeuille soit en possession des attestations de clé nécessaires à la délivrance des données d'identification personnelle et des attestations électroniques d'attributs liées à un appareil.

([3]) ETSI, "Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 3: JAdES levels and baseline profiles", ETSI TS 119 472-3, V1.1.1, mars 2026.

— TR_KA-3: en cas de nécessité lors de la délivrance, une unité de portefeuille doit contenir une attestation de clé dans le champ 'proofs' d'une demande de justificatif d'identité adressée à l'émetteur de justificatifs d'identité, comme indiqué dans la spécification OID4VCI, dans une preuve de type 'jwt' ou de type 'attestation'.

— TR_KA_3.1: lorsqu'une unité de portefeuille comprend une attestation de clé dans un élément 'jwt', elle doit apposer une signature ou un cachet sur l'attestation de clé en utilisant la clé privée correspondant à la clé publique située à l'index 0 du tableau 'attested_keys' dans l'objet 'key_attestation'.

— TR_KA-4: lorsqu'un émetteur de justificatifs d'identité émet des justificatifs liés à un appareil, il doit indiquer dans le paramètre 'proof_types_supported' de ses métadonnées, comme spécifié à la section 12.2.4 de la spécification OID4VCI, qu'il prend en charge à la fois le type de preuve 'jwt' et le type de preuve 'attestation' pour les attestations de clé qui contiennent l'objet 'key_attestations_required'.

— TR_KA-4.1: lorsqu'un émetteur de justificatifs d'identité délivre des justificatifs non liés à un appareil, il doit omettre les paramètres 'proof_types_supported' et 'cryptographic_binding_methods_supported' dans ses métadonnées d'émetteur de justificatifs d'identité.

— TR_KA-5: lorsqu'un émetteur de justificatifs d'identité reçoit une attestation de clé dans un type de preuve 'jwt' ou 'attestation', il doit vérifier la signature de l'attestation de clé en utilisant la clé publique contenue dans le certificat de signature inclus dans le paramètre 'x5c' de l'en-tête JOSE de l'attestation de clé et s'assurer que ce certificat de signature est relié à une ancre de confiance figurant sur la liste des fournisseurs de portefeuille visée à l'article 5 du règlement d'exécution (UE) 2024/2980, en utilisant éventuellement des certificats intermédiaires inclus dans le paramètre 'x5c'.

— TR_KA-6: lorsqu'un émetteur de justificatifs d'identité reçoit une attestation de clé dans un type de preuve 'jwt', il doit vérifier la signature de l'élément 'jwt' en utilisant la clé située à l'index 0 du tableau 'attested_keys' dans l'objet 'key_attestation' inclus dans l'élément 'jwt'.

— TR_KA-6.1: l'émetteur de justificatifs d'identité doit vérifier que le champ 'nonce' de l'élément 'jwt' comprend un c_nonce valide obtenu depuis son nonce_endpoint, comme indiqué dans la spécification OID4VCI.

— TR_KA-7: lorsqu'un émetteur de justificatifs d'identité reçoit une attestation de clé dans un type de preuve 'attestation', il doit vérifier que l'objet 'key_attestation' contient un c_nonce valide obtenu depuis son nonce_endpoint.

— TR_KA-8: un fournisseur de données d'identification personnelle doit veiller à ce que les données d'identification personnelle soient reliées à une clé publique provenant d'une attestation de clé mentionnant un WSCD.

c) Exigences en matière de contenu

— C_WIA-1: une attestation d'instance de portefeuille doit comprendre les éléments suivants:

— la revendication 'wallet_name' définie à l'appendice E de la spécification OID4VCI, dont la valeur doit être l'identifiant de la solution de portefeuille qui figure sur la liste des fournisseurs de portefeuille visée à l'article 5 du règlement d'exécution (UE) 2024/2980;

— une revendication 'wallet_version' ([4]), qui doit être une chaîne de caractères dont la valeur doit être la version de la solution de portefeuille;

— une revendication 'wallet_solution_certification_information', qui doit être un objet JSON contenant des informations sur l'organisme d'évaluation de la conformité qui a certifié la solution de portefeuille, le numéro de certification, le cas échéant, et d'autres informations pertinentes concernant la certification;

([4]) Cette revendication est définie dans le présent règlement d'exécution de la Commission car elle ne fait partie de la spécification OID4VCI.

— une revendication 'client_status', contenant deux sous-champs:

— 'status': une référence à la liste d'états telle que définie à l'appendice E de la spécification OID4VCI, qui représente l'état de révocation de l'instance de portefeuille. Voir la section e) ci-dessous pour plus de détails;

— 'exp': une NumericDate, telle que spécifiée dans la RFC 7519, indiquant jusqu'à quel moment le fournisseur de portefeuille maintiendra l'état de révocation à l'index de la liste d'états référencé dans le champ 'status';

— la revendication 'exp' définie à l'appendice E de la spécification OID4VCI.

— *REMARQUE:* la revendication 'client_status.status' dans une attestation d'instance de portefeuille représente l'état de révocation de l'instance de portefeuille, et non l'état de révocation de l'attestation elle-même. Comme décrit dans le paragraphe R_WIA-1 ci-dessous, un fournisseur de portefeuille peut décider de limiter la portée de chaque attestation d'instance de portefeuille à un serveur d'autorisation spécifique en se fondant sur le fait que toutes les attestations envoyées à ce serveur contiennent la même valeur d'index dans l'entrée 'client_status.status'.

— *REMARQUE:* la valeur 'idx' dans la revendication 'status' peut être utilisée comme identifiant unique (pairwise) de l'instance de portefeuille et de l'unité de portefeuille.

— C_WIA-2: une attestation d'instance de portefeuille devrait comprendre également la revendication 'wallet_link' définie à l'appendice E de la spécification OID4VCI, la valeur de cette revendication étant un URI permettant d'obtenir des informations supplémentaires sur la solution de portefeuille.

— C_WIA-3: un serveur d'autorisation ne doit pas interpréter le paramètre 'exp' au niveau le plus élevé d'une attestation d'instance de portefeuille comme étant la fin de la période de maintien de la révocation de l'instance de portefeuille.

— *REMARQUE:* le paramètre 'exp' au niveau le plus élevé d'une attestation d'instance de portefeuille indique à quel moment l'attestation proprement dite expire.

— C_KA-1: une attestation de clé comprend:

— les revendications 'key_storage' et 'user_authentification' définies à l'appendice D de la spécification OID4VCI.

— Les attributs 'key_storage' et 'user_authentification' doivent avoir la valeur 'iso_18045_high' lorsqu'une attestation de clé mentionne un WSCD;

— la revendication "certification" définie à l'appendice D de la spécification OID4VCI, contenant une URL permettant d'obtenir des informations sur la certification obtenue par le WSCD ou le magasin de clés, à titre indicatif le schéma tel que Common Criteria ou GlobalPlatform, les exigences évaluées telles que le profil de protection applicable et le niveau d'évaluation.

— Ces informations permettent de déterminer si le stockage de la clé est un WSCD;

— une revendication 'key_storage_status', contenant deux sous-champs:

— 'status': une référence à la liste d'états telle que définie à l'appendice D.1 de la spécification OID4VCI. La valeur représente soit l'état de révocation du WSCD ou du type de magasin de clés utilisé pour stocker les clés attestées, soit, dans le cadre de l'option d'index per-key-attestation, l'état de révocation du WSCD ou du magasin de clés d'une unité de portefeuille individuelle. Voir R_KA_1 ci-dessous pour les options d'attribution d'index disponibles;

— 'exp': une NumericDate, telle que spécifiée dans la RFC 7519, indiquant jusqu'à quel moment le fournisseur de portefeuille maintiendra l'état de révocation à l'index de la liste d'états référencé dans le champ 'status';

— la revendication 'exp' définie à l'appendice D de la spécification OID4VCI.

— *REMARQUE* concernant la valeur 'idx' dans la revendication 'key_storage_status.status' d'une attestation de clé: lorsque le fournisseur de portefeuille utilise l'option 'type-shared index' (voir R_KA_1 ci-dessous), toutes les attestations de clé se rapportant au même type de WSCD ou de magasin de clés partagent le même index de la liste d'états. Par conséquent, la valeur 'idx' n'est pas unique pour chaque unité de portefeuille. À l'inverse, lorsque le fournisseur de portefeuille utilise l'option 'per-key-attestation index', la valeur 'idx' est unique pour chaque unité de portefeuille (ou unique en mode 'pairwise' pour chaque émetteur de justificatifs d'identité). Toutefois, dans tous les cas, un émetteur de justificatifs d'identité ne doit pas utiliser la valeur 'idx' dans une attestation de clé comme identifiant d'unité de portefeuille, mais doit utiliser plutôt la valeur 'idx' dans une attestation d'instance de portefeuille.

— C_KA-2: lorsqu'une attestation de clé est envoyée dans un type de preuve 'attestation', elle doit également comprendre un c_nonce valide, tel que défini à l'appendice F.3 de la spécification OID4VCI.

— C_KA-3: un émetteur de justificatifs d'identité ne doit pas interpréter le paramètre 'exp' au niveau le plus élevé d'une attestation de clé comme étant la fin de la période de maintien de la révocation du WSCD ou du magasin de clés.

— *REMARQUE:* le paramètre 'exp' au niveau le plus élevé d'une attestation de clé indique à quel moment l'attestation de clé proprement dite expire.

d) Exigences relatives au cycle de vie

— La présente annexe spécifie les paramètres de métadonnées suivants de l'émetteur de justificatifs d'identité:

— 'preferred_client_status_period': FACULTATIF. Un nombre entier indiquant la durée restante préférée de maintien de l'état de l'attestation d'instance de portefeuille à présenter par l'unité de portefeuille lors de la délivrance, en secondes. La durée restante de maintien de l'état est définie comme la valeur de 'client_status.exp' dans l'attestation, moins l'heure de réception de l'attestation.

— 'preferred_key_storage_status_period': FACULTATIF. Un nombre entier indiquant la durée restante préférée de maintien de l'état de l'attestation de clé à présenter par l'unité de portefeuille lors de la délivrance, en secondes. La durée restante de maintien de l'état est définie comme la valeur de 'key_storage_status.exp' dans l'attestation, moins l'heure de réception de l'attestation.

— LC_WIA-1: un serveur d'autorisation peut communiquer ses préférences en ce qui concerne la durée restante de maintien de l'état dans les attestations d'instance de portefeuille en intégrant le paramètre de métadonnées 'preferred_client_status_period' dans son point de terminaison de métadonnées d'émetteur de justificatifs d'identité, comme indiqué à la section 12.2.2 de la spécification OID4VCI.

— LC_WIA-1.1: ce champ doit être placé au niveau le plus élevé des métadonnées de l'émetteur de justificatifs d'identité.

— LC_WIA_2: un serveur d'autorisation ne doit pas interpréter le paramètre 'exp' au niveau le plus élevé d'une attestation d'instance de portefeuille comme étant la fin de la période de maintien de la révocation de l'instance de portefeuille.

— LC_WIA_3: lorsqu'un fournisseur de portefeuille appose sa signature ou son cachet sur une attestation d'instance de portefeuille, il doit maintenir l'état de révocation de l'instance de portefeuille concernée jusqu'à ce que la 'wallet_instance_status.exp' indiquée dans cette attestation d'instance de portefeuille soit écoulée.

— LC_KA-1: si une attestation de clé est nécessaire, un émetteur de justificatifs d'identité peut communiquer ses préférences en ce qui concerne la durée restante de maintien de l'état dans les attestations de clé en intégrant le paramètre de métadonnées spécifié plus haut 'preferred_key_storage_status_period' dans son point de terminaison de métadonnées d'émetteur de justificatifs d'identité, comme indiqué à la section 12.2.2 de la spécification OID4VCI.

— LC_KA-1.1: ce champ doit être placé à l'intérieur de l'objet 'key_attestations_required' comme indiqué à la section 12.2.4 de la spécification OID4VCI.

— LC_KA-2: un fournisseur de portefeuille doit choisir la période de validité technique des attestations de clé qu'il délivre.

— LC_KA-3: lorsqu'un fournisseur de portefeuille appose sa signature ou son cachet sur une attestation de clé, il doit maintenir l'état de révocation du WSCD ou du magasin de clés jusqu'à ce que la 'key_storage_status.exp' indiquée dans cette attestation de clé soit écoulée.

— LC_GEN-1: un fournisseur de portefeuille doit veiller à ce qu'une unité de portefeuille puisse toujours présenter des attestations d'unité de portefeuille et des attestations de clé dont les 'client_status.exp' et 'key_storage_status.exp' (respectivement) sont situées au moins 31 jours plus tard au moment de leur présentation à un serveur d'autorisation ou à un émetteur de justificatifs d'identité.

— *REMARQUE:* cela garantit que les fournisseurs de données d'identification personnelle peuvent s'appuyer sur un chaînage de révocation sans être contraints de délivrer des données d'identification personnelle à courte durée de vie.

— LC_GEN-2: un fournisseur de portefeuille doit veiller à ce qu'une unité de portefeuille récupère les métadonnées de l'émetteur de justificatifs d'identité lors de la délivrance.

  — LC_GEN_2.1: si un champ 'preferred_key_storage_status_period' est inclus dans ces métadonnées, l'unité de portefeuille doit envoyer une attestation de clé pour laquelle la valeur ('key_storage_status.exp' − date actuelle) − 'preferred_key_storage_status_period' est la plus proche possible de zéro sans être négative. Si l'unité de portefeuille ne dispose pas d'une telle attestation de clé, elle doit obtenir du fournisseur de portefeuille une nouvelle attestation de clé qui satisfait à la condition 'key_storage_status.exp' − date actuelle ≥ 'preferred_key_storage_status_period'.

  — LC_GEN_2.2: si un champ 'preferred_client_status_period' est inclus dans ces métadonnées, l'unité de portefeuille doit envoyer une attestation d'instance de portefeuille pour laquelle la valeur ('client_status.exp' − date actuelle) − 'preferred_client_status_period' est la plus proche possible de zéro sans être négative. Si l'unité de portefeuille ne dispose pas d'une telle attestation d'instance de portefeuille, elle doit obtenir du fournisseur de portefeuille une nouvelle attestation d'instance de portefeuille qui satisfait à la condition 'client_status.exp' − date actuelle ≥ 'preferred_client_status_period'.

— LC_GEN-3: la période de validité technique des données d'identification personnelle doit prendre fin avant le 'client_status.exp' de l'attestation d'instance de portefeuille et avant le 'key_storage_status.exp' de l'attestation de clé envoyées au fournisseur de données d'identification personnelle lors du processus de délivrance.

— LC_GEN-4: un fournisseur de données d'identification personnelle ayant une période de validité technique de plus de 24 heures doit vérifier l'état de révocation de l'attestation d'instance de portefeuille et de l'attestation de clé reçues lors de la délivrance au moins une fois toutes les 24 heures pendant la période de validité technique des données d'identification personnelle. Lorsque l'une ou l'autre de ces attestations est révoquée, le fournisseur doit révoquer les données d'identification personnelle.

e) Exigences en matière de révocation

— R_GEN-1: un fournisseur de portefeuille doit utiliser des listes d'états des jetons (définies dans la spécification Token Status List de l'IETF) comme mécanisme de révocation tant pour les attestations de clé que pour les attestations d'instance de portefeuille, comme indiqué respectivement dans les appendices D et E de la spécification OID4VCI.

— *REMARQUE:* pour améliorer la modularité de ses listes d'états, un fournisseur de portefeuille peut recourir aux optimisations suivantes:

  — diviser la liste d'états en plusieurs sections, lorsque les fournisseurs de portefeuille comptent un nombre important d'utilisateurs et d'attestations délivrées. Il existe beaucoup de stratégies de sectionnement, fondées par exemple sur une taille fixe ou sur une période donnée. La stratégie de sectionnement est laissée à l'appréciation du fournisseur de portefeuille. Les critères à prendre en considération peuvent comprendre la taille des listes d'états à télécharger et le respect de la vie privée de l'utilisateur;

  — prévoir plusieurs listes d'états;

  — comprimer les listes d'états pour en réduire la taille.

— R_WIA-1: un fournisseur de portefeuille peut attribuer la même valeur à la revendication 'idx' dans la revendication 'client_status.status' de toutes les attestations d'instance de portefeuille qu'une unité de portefeuille donnée présente au même serveur d'autorisation. Cette option est appelée 'per-issuer reuse'. Si cette option est utilisée, les conditions suivantes s'appliquent:

  — R_WIA-1.1: l'unité de portefeuille doit conserver la trace de la valeur d'index qu'elle a utilisée pour chaque serveur d'autorisation avec lequel elle a précédemment interagi et doit demander une attestation d'instance de portefeuille contenant cette même valeur d'index lorsqu'elle interagit à nouveau avec le même serveur d'autorisation.

  — R_WIA-1.2: lorsqu'un fournisseur de portefeuille reçoit une demande d'attestation d'instance de portefeuille contenant une valeur d'index spécifique, il doit vérifier que l'unité de portefeuille à l'origine de la demande a reçu cette valeur d'index au préalable avant de délivrer une nouvelle attestation d'instance de portefeuille avec cette valeur d'index.

  — R_WIA-1.3: l'unité de portefeuille ne doit pas réutiliser la même valeur d'index pour ses interactions avec d'autres serveurs d'autorisation.

— *REMARQUE:* si l'option 'per-issuer reuse' est utilisée, le fournisseur de portefeuille sera en mesure de déterminer le nombre de serveurs d'autorisation avec lesquels une unité de portefeuille a interagi et la fréquence à laquelle elle interagit avec chacun d'eux.

— R_WIA-2: dans sa politique relative au respect de la vie privée, le fournisseur de portefeuille doit indiquer s'il utilise l'option 'per-issuer reuse' pour la révocation des instances de portefeuille.

— R_WIA-3: si un fournisseur de portefeuille n'utilise pas l'option 'per-issuer reuse', il doit attribuer une valeur d'index nouvelle et non associable à chaque attestation d'instance de portefeuille qu'il délivre.

— R_WIA-4: si une unité de portefeuille doit être révoquée, le fournisseur de portefeuille doit révoquer les valeurs d'index dans la revendication 'client_status.statu' de toutes les attestations d'instance de portefeuille associées à cette unité de portefeuille.

— R_WIA-5: un fournisseur de portefeuille doit tenir compte de l'échelle de son déploiement et de l'architecture sous-jacente lorsqu'il détermine la taille des listes d'états de ses attestations d'instance de portefeuille, en veillant à ce qu'elles soient suffisamment grandes pour empêcher la corrélation et protéger la vie privée des utilisateurs. Dans la mesure du possible, une liste d'états doit se rapporter au minimum à 10 000 attestations.

— R_KA_1: un fournisseur de portefeuille doit choisir l'une des options d'assignation d'index suivantes pour la revendication 'key_storage_status.status' dans une attestation de clé:

  — option 1, appelée 'type-shared index', dans laquelle toutes les attestations de clé attestant des clés stockées dans le même type de WSCD ou de magasin de clés contiennent la même valeur d'index dans 'key_storage_status.status';

  — option 2, appelée 'per-key-attestion index', dans laquelle une attestation de clé attestant des clés stockées dans un WSCD donné ou un magasin de clés donné contient une valeur d'index unique (pairwise) dans 'key_storage_status.status'.

— *REMARQUE:* lorsqu'un fournisseur de portefeuille utilise l'option 1, une action de révocation unique annule toutes les attestations de clés du type concerné pour toutes les unités de portefeuille. En outre, étant donné que toutes les attestations de clé pour un même type de WSCD ou de magasin de clés partagent un index unique de la liste d'états, le nombre d'entrées dans cette liste pour une attestation de clé correspond au nombre de types de WSCD ou de magasins de clés pris en charge par le fournisseur de portefeuille, et non au nombre d'unités de portefeuille déployées. Par conséquent, les considérations relatives à la protection de la vie privée qui motivent la taille minimale de la liste d'états dans le cas des instances de portefeuille ne s'appliquent pas aux listes d'états des attestations de clé dans le cadre de l'option 1, à condition qu'un nombre suffisant d'unités de portefeuille utilise le même type de WSCD ou de magasin de clés.

— *REMARQUE:* lorsqu'un fournisseur de portefeuille utilise l'option 2, chaque index représente l'état de révocation du WSCD ou du magasin de clés spécifique attesté dans cette attestation de clé.

— *REMARQUE:* lorsqu'un fournisseur de portefeuille utilise l'option 2, un WSCD ou un magasin de clés spécifique peut également être révoqué à la demande de l'utilisateur.

— R_KA-2: lorsqu'un fournisseur de portefeuille utilise l'option 2, il peut, à titre facultatif, utiliser l'option 'per-issuer reuse' décrite dans le paragraphe R_WIA-1. Si le fournisseur de portefeuille utilise cette option, les exigences des paragraphes R_WIA-1 à R_WIA-3 s'appliquent par analogie.

— R_KA-3: si un fournisseur de portefeuille utilise l'option 2, il doit tenir compte de l'échelle de son déploiement et de l'architecture sous-jacente lorsqu'il détermine la taille des listes d'états de ses attestations de clé, en veillant à ce qu'elles soient suffisamment grandes pour empêcher la corrélation et protéger la vie privée des utilisateurs. Dans la mesure du possible, une liste d'états doit se rapporter au minimum à 10 000 attestations de clé.

— R_KA-4: si un fournisseur de portefeuille utilise l'option 1 ('type-shared index'), il ne doit révoquer une entrée 'key_storage_status.status' que si le type de WSCD ou de magasin de clés présente une vulnérabilité en matière de sécurité.

f) Exigences relatives aux algorithmes de signature

— SA-1: pour signer les attestations d'instance de portefeuille, les attestations de clé, les preuves de possession connexes et les listes d'états des jetons, l'un des algorithmes suivants doit être utilisé:

  — ES256 (ECDSA avec SHA-256 et P-256)

  — ES384 (ECDSA avec SHA-384 et P-384)

  — ES512 (ECDSA avec SHA-512 et P-521)

— SA-2: un fournisseur de portefeuille doit choisir lequel des algorithmes mentionnés dans le paragraphe SA-1 il utilisera.

— SA-3: un serveur d'autorisation ou un émetteur de justificatifs d'identité (tels que définis dans la spécification OID4VCI) doit prendre en charge tous les algorithmes mentionnés dans le paragraphe SA-1.».

ANNEXE IV

«*ANNEXE II*

Liste des normes visées à l'article 8

Les spécifications techniques énoncées dans les paragraphes 2 à 6 d'ETSI TS 119 472-1 V1.2.1 (2026-02) s'appliquent, moyennant les adaptations suivantes:

1) 2.1. Références normatives

— [16] ETSI EN 319 412-1 V1.6.1 (2025-06): "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures (Signatures électroniques et infrastructures de confiance (ESI) - profils de certificat; partie 1: présentation générale et structures de données communes)".

— [17] ETSI TS 119 412-6 V1.1.1 (2025-09): "Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 6: Certificate profile requirements for PID, Wallet, EAA, QEAA, and PSBEAA providers [Signatures électroniques et infrastructures de confiance (ESI); profils de certificat; partie 6: Exigences applicables aux profils de certificats pour les fournisseurs de données d'identification personnelle (PID), de portefeuilles, d'attestations électroniques d'attributs (EAA), d'attestations électroniques qualifiées d'attributs (QEAA) et d'attestations électroniques d'attributs délivrées par un organisme du secteur public (PSBEAA)]".

— [25] Token Status List (TSL) de l'IETF, draft-ietf-oath-status-list-20: "Token Status List", 20 avril 2026.

2) 4.2.11.1 General requirements

— EAA-4.2.11.1-06: lorsqu'un élément d'état est utilisé pour des données d'identification personnelle, des attestations électroniques qualifiées d'attributs ou des attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte, il indique uniquement si l'attestation est révoquée ou non et ne prend en charge aucune autre valeur d'état telle que la suspension.

— EAA-4.2.11.1-06.1: lorsqu'une attestation est révoquée, sa révocation est permanente.

3) 4.2.13 EAA short-lived

— EAA-4.2.13-03: lorsque des attestations électroniques d'attributs à faible durée de validité sont délivrées pour 24 heures ou moins, aucune révocation n'est exigée.

4) 4.6.3. Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (PuB-EAA)

— PuB-EAA-4.6.2-03: vide.

— Pub-EAA-4.6.2-04: vide.

— PuB-EAA-4.6.3-03: La signature numérique PuB-EAA devrait contenir le certificat qualifié à l'appui de la signature numérique PuB-EAA.

— PuB-EAA-4.6.3-04: Le certificat qualifié à l'appui de la signature numérique PuB-EAA doit satisfaire aux exigences du paragraphe 8 d'ETSI TS 119 412-6 v1.1.1 et doit contenir le QcType qcStatement tel que défini dans ETSI EN 319 412-5 v2.5.1, la valeur id-etsi-qct-eidaspsbeaa étant définie comme suit:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER: = {id-etsi-eidas2-qct-extensions 3} — Certificat visé à l'article 45 *septies*, paragraphe 1, point b), à l'appui de la signature électronique qualifiée ou du cachet électronique qualifié de l'organisme du secteur public visé à l'article 3, point 46), du règlement (UE) n° 910/2014.

5) 5.2.10.1 General requirements

— EAA-5.2.10.1-04: vide.

— EAA-5.2.10.1-05: vide.

— EAA-5.2.10.1-06: Le membre "status" peut contenir le membre "status_list" comme indiqué au paragraphe 6.2 du projet draft-ietf-oauth-status-list-20 de l'IETF[25].

— EAA-5.2.10.1-07: vide.

— EAA-5.2.10.1-08: vide.

— EAA-5.2.10.1-09: vide.

— EAA-5.2.10.1-10: vide.

— EAA-5.2.10.1-11: vide.

— EAA-5.2.10.1-12: vide.

6) 6.2.10.1 General requirements

— EAA-6.2.10.1-01: lorsqu'une attestation électronique d'attributs conforme à la norme ISO/IEC mdoc utilise le mécanisme de liste d'états d'attestations tel que défini dans EAA-6.2.10.1-02.2 ou le mécanisme de liste de révocation d'attestations tel que défini dans EAA-6.2.10.1-02.3, son objet de sécurité mobile (MSO) contient la structure d'état, telle que spécifiée dans EAA-6.2.10.1-17, qui contient les informations de révocation du MSO.

— EAA-6.2.10.1-01.1: lorsque l'élément d'état met en œuvre le mécanisme de liste d'identifiants, il contient l'élément identifier_list figurant dans EAA-6.2.10.1-11.

— EAA-6.2.10.1-01.2: lorsque l'élément d'état met en œuvre le mécanisme de liste d'états, il contient l'élément status_list figurant dans EAA-6.2.10.1-13.

— *REMARQUE:*

  — La structure d'état contient une référence à une liste de révocation de MSO.

  — La liste de révocation de MSO est une structure COSE_Sign1 qui indique si un MSO donné est révoqué ou non.

  — La structure d'état contient toutes les informations nécessaires pour permettre à la partie utilisatrice de portefeuille de déterminer si la liste de révocation de MSO est authentique.

— EAA-6.2.10.1-02: le fournisseur de données d'identification personnelle, le fournisseur d'attestations électroniques d'attributs qualifiées ou le fournisseur d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte utilise l'une des méthodes suivantes pour la révocation des données d'identification personnelle, des attestations électroniques d'attributs qualifiées ou des attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte:

— EAA-6.2.10.1-02.1: lorsqu'il délivre des attestations électroniques d'attributs à faible durée de validité pour une période inférieure ou égale à 24 heures, la révocation n'est pas nécessaire.

— EAA-6.2.10.1-02.2: utiliser un mécanisme de liste d'états d'attestation pour encoder les informations de révocation sous forme de liste d'états.

— EAA-6.2.10.1-02.2.1: le mécanisme de liste d'états révoque un MSO si le bit de la position de bit définie par l'émetteur dans le MSO est activé dans la liste d'états.

— EAA-6.2.10.1-02.2.2: le mécanisme de liste d'états est précisé dans la spécification relative à la liste d'états des jetons (draft-ietf-oauth-status-list-20).

— EAA-6.2.10.1-02.3: utiliser un mécanisme de liste de révocation d'attestations pour encoder les informations de révocation sous forme de liste d'identifiants.

— EAA-6.2.10.1-02.3.1: le mécanisme de liste d'identifiants révoque un MSO si l'identifiant défini par l'émetteur dans le MSO figure sur la liste d'identifiants.

— EAA-6.2.10.1-02.3.2: EAA-6.2.10.1-06, EAA-6.2.10.1-08, EAA-6.2.10.1-09, EAA-6.2.10.1-10 et EAA-6.2.10.1-11 précisent le mécanisme de liste d'identifiants, sur la base des exigences de la spécification relative à la liste d'états des jetons, y compris les points communs entre le mécanisme de liste d'états et le mécanisme de liste d'identifiants.

— EAA-6.2.10.1-03: lorsqu'un élément d'état est utilisé pour des données d'identification personnelle, des attestations électroniques qualifiées d'attributs ou des attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte, l'état "révoqué" doit être utilisé exclusivement.

— EAA-6.2.10.1-03.1: pour une liste d'états, cela signifie que seules les valeurs 'valid' et 'invalid', telles que précisées dans la spécification relative à la liste d'états des jetons, doivent être utilisées.

— EAA-6.2.10.1-03.2: pour la liste d'identifiants, seuls les MSO révoqués, par opposition aux MSO provisoirement suspendus, doivent être inscrits sur la liste d'identifiants.

— EAA-6.2.10.1-04: lorsqu'un MSO est révoqué, sa révocation est permanente.

— EAA-6.2.10.1-05: la vérification de la liste de révocation du MSO est facultative pour la partie utilisatrice de portefeuille et, le cas échéant, la vérification doit être conforme aux exigences de vérification précisées dans la spécification relative à la liste d'états des jetons et la spécification relative à la structure d'état énoncée dans EAA-6.2.10.1-01.

— EAA-6.2.10.1-05.1: lorsqu'une partie utilisatrice de portefeuille doit être en mesure de vérifier l'état de révocation des données d'identification personnelle ou des attestations électroniques d'attributs, elle doit prendre en charge à la fois le mécanisme de liste d'états d'attestations et le mécanisme de liste de révocation d'attestations prévus dans EAA-6.2.10.1-02.

— EAA-6.2.10.1-06: le identifier_list et le status_list du MSO peuvent contenir l'élément de certificat.

— EAA-6.2.10.1-06.1: lorsque l'élément de certificat est présent, il doit contenir un certificat contenant la clé publique ayant apposé la signature ou le cachet sur le certificat de plus haut niveau dans l'élément x5chain de la structure de liste de révocation du MSO.

— EAA-6.2.10.1-06.1.1: la partie utilisatrice de portefeuille doit utiliser ce certificat comme ancre de confiance pour vérifier l'élément x5chain de la structure de liste de révocation du MSO.

— EAA-6.2.10.1-06.2: en l'absence d'élément de certificat, le certificat avec lequel a été signé le certificat dans l'élément x5chain du MSO doit être utilisé pour apposer la signature ou le cachet sur le certificat de niveau supérieur dans l'élément x5chain de la structure de liste de révocation du MSO.

— EAA-6.2.10.1-06.2.1: l'instance de la partie utilisatrice de portefeuille doit utiliser ce certificat comme ancre de confiance pour vérifier l'élément x5chain de la structure de liste de révocation du MSO.

— EAA-6.2.10.1-07: conformément à la spécification de liste d'états des jetons, une liste de révocation du MSO doit être mise en œuvre sous forme de jeton de liste d'états au format CWT.

— EAA-6.2.10.1-08: pour la liste de révocation du MSO: pour le mécanisme de la liste d'identifiants et le mécanisme de liste d'états, les exigences applicables sont les suivantes:

  — la revendication exp doit être présente.

  — la revendication ttl doit être présente.

  — la revendication aggregation_uri dans la revendication IdentifierList ou StatusList peut être présente et le fournisseur de données d'identification personnelle, le fournisseur d'attestations électroniques qualifiées d'attributs ou le fournisseur d'attestations électroniques d'attributs délivrées par un organisme du secteur

public responsable d'une source authentique ou pour son compte peut utiliser la revendication aggregation_uri pour indiquer que le mécanisme d'agrégation tel que spécifié dans la spécification de la liste d'états des jetons est pris en charge.

— le CWT doit être un objet COSE_Sign1 utilisant l'un des algorithmes de signature suivants pour calculer la signature:

a) 'ES256' (ECDSA avec courbe NIST P-256 et SHA-256);

b) 'ES384' (ECDSA avec courbe NIST P-384 et SHA-384);

c) 'ES512' (ECDSA avec courbe NIST P-521 et SHA-512);

d) 'ESB256' (ECDSA avec courbe NIST brainpoolP256r1 et SHA-256);

e) 'ESB384' (ECDSA avec courbe NIST brainpoolP384r1 et SHA-384);

f) 'ESB512' (ECDSA avec courbe NIST brainpoolP512r1 et SHA-512);

— le CWT doit contenir la x5chain dans l'en-tête protégé qui contient le certificat ou la chaîne de certificats afin de vérifier la signature de la liste de révocation du MSO.

— l'utilisation étendue de la clé de l'identifiant d'objet précisé dans la spécification de la liste d'états des jetons peut servir au certificat de signature de la liste d'états et au certificat de signature de la liste d'identifiants et les instances de parties utilisatrices de portefeuille peuvent prendre en charge l'utilisation étendue de la clé des identifiants d'objet précisés dans la spécification de la liste d'états des jetons et pour l'identifiant d'objet, le fournisseur d'attestations électroniques d'attributs qualifiées ou le fournisseur d'attestations électroniques d'attributs délivrées par un organisme du secteur public ou pour son compte ne doivent pas rendre critique le champ d'utilisation étendue de la clé lorsqu'ils utilisent l'OID d'utilisation étendue de la clé précisé dans la spécification de la liste d'états des jetons.

— EAA-6.2.10.1-09: par dérogation aux exigences de la spécification de la liste d'états des jetons, pour le mécanisme de liste d'identifiants, les exigences applicables sont les suivantes:

— la valeur de la revendication type doit être 'application/identifierlist+cwt';

— la revendication StatusList ne doit pas être présente dans l'ensemble de revendications CWT;

— la structure IdentifierList définie dans EAA-6.2.10.1-11 doit être présente en tant que revendication dans l'ensemble de revendications CWT qui utilise la clé 65530.

— EAA-6.2.10.1-10: la structure IdentifierList doit être une structure CBOR avec le CDDL suivant:

```
IdentifierList = {

    'identifiers': { * Identifier => IdentifierInfo },

    ? 'aggregation_uri': Aggregation_uri

    * tstr => RFU

}

IdentifierInfo = { tstr/int => RFU }

Identifier = bstr

Aggregation_uri = tstr
```

— EAA-6.2.10.1-10.1: lorsque l'identifiant dans la IdentifierList est présent, le MSO qui contient l'identifiant dans l'élément d'état est révoqué.

— EAA-6.2.10.1-10.2: la revendication aggregation_uri est précisée dans la section 9.2 de la spécification de la liste d'états des jetons.

— EAA-6.2.10.1-10.3: le type de contenu de la liste d'identifiants doit être 'application/identifierlist+cwt' tel qu'énoncé dans les exigences figurant dans la section 8.2 de la spécification de la liste d'états des jetons.

— EAA-6.2.10.1-11: les exigences applicables à l'élément identifier_list dans le MSO sont les suivantes (voir EAA-6.2.10.1-17).

— EAA-6.2.10.1-11.1: l'élément identifier_list est une structure CBOR avec le CDDL suivant:

```
IdentifierListInfo = {

        'id': Identifier ,

        'uri': URI,

        ? 'certificate': Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: pour éviter toute éventuelle utilisation de l'identifiant comme corrélation dans différentes présentations, il doit être unique pour chaque MSO.

— EAA-6.2.10.1-12: les exigences applicables à la liste d'états sont les suivantes:

  — EAA-6.2.10.1-12.1: l'élément bits de la structure de StatusList doit être fixé à 1.

— EAA-6.2.10.1-13: les exigences applicables à l'élément status_list dans le MSO sont les suivantes (voir EAA-6.2.10.1-17).

  — EAA-6.2.10.1-13.1: l'élément status_list doit respecter les exigences applicables à la structure StatusListInfo précisées dans la spécification relative à la liste d'états des jetons et l'élément de certificat facultatif défini dans EAA-6.2.10.1-06 doit être ajouté.

  — EAA-6.2.10.1-13.2: pour éviter toute éventuelle utilisation de l'index d'état comme corrélation dans différentes présentations, chaque MSO doit avoir une combinaison d'index d'état et d'URI unique.

— EAA-6.2.10.1-14: le fournisseur de portefeuille doit utiliser la deuxième (EAA-6.2.10.1-02.2) ou la troisième (EAA-6.2.10.1-02.3) des méthodes spécifiées dans EAA-6.2.10.1-02 pour la révocation d'une attestation d'instance de portefeuille (WIA) et pour la révocation d'une attestation de clé (KA).

— EAA-6.2.10.1-15: le fournisseur de portefeuille met en œuvre les mécanismes de révocation d'attestation spécifiés dans EAA-6.2.10.1-02 dans sa solution de portefeuille.

— EAA-6.2.10.1-16: le fournisseur de données d'identification personnelle et le fournisseur d'attestations électroniques d'attributs doivent prendre en charge à la fois le mécanisme de liste d'états d'attestations et le mécanisme de liste de révocation d'attestations spécifiés dans EAA-6.2.10.1-02 pour vérifier l'état de révocation d'une attestation d'instance de portefeuille (WIA) et d'une attestation de clé (KA).

— EAA-6.2.10.1-17: la structure d'état dans le MSO doit être une structure CBOR avec le CDDL suivant:

```
Status = {
? 'identifier_list' : IdentifierListInfo,
? 'status_list': StatusListInfo,
* tstr => RFU
    }»
```

ANNEXE V

«ANNEXE III

Spécifications techniques visées à l'article 10

— Spécifications techniques:

  — paragraphe 4.2.5 de l'ETSI TS 119 472-3 V1.1.1 (2026-03).»

ANNEXE VI

L'annexe IV du règlement d'exécution (UE) 2024/2979 est modifiée comme suit:

1) Le point 1 est remplacé par le texte suivant:

«1. Format de signature ou de cachet obligatoire:

a) PAdES (PDF Advanced Electronic Signature) comme spécifié dans ETSI EN 319 142-1 V1.2.1 (2024-01); "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures [Signatures électroniques et infrastructures de confiance (ESI) - Signatures numériques PAdES; partie 1: blocs de base et signatures de référence PAdES]."».

2) Le point 3 est remplacé par le texte suivant:

«3. Interface de programmation d'application:
ETSI TS 119 432 v1.3.1 (2026-03) paragraphes 6.4.3, A.6, A.7 et A.8.».

ANNEXE VII

«*ANNEXE VI*

Label de confiance de l'UE pour le portefeuille d'identité numérique en couleur



»

ANNEXE VIII

«*ANNEXE VII*

Label de confiance de l'UE pour le portefeuille d'identité numérique en noir et blanc



»

ANNEXE IX

«ANNEXE VIII

Données du label de confiance de l'UE pour le portefeuille d'identité numérique

Données	Description	Encodage	Statut
TrustMarkResourceURL	URL des ressources graphiques du label de confiance de l'UE pour le portefeuille d'identité numérique et des ressources d'information des utilisateurs dans l'interface utilisateur du portefeuille.	URL	Obligatoire
ListOfCertifiedWalletsURL	URL de la liste publique des solutions de portefeuille certifiées dans l'UE, telle que prévue par le règlement d'exécution (UE) 2025/849 de la Commission ([1]).	URL	Obligatoire
ListOfCertifiedWalletsQRCode	Code QR contenant les informations de ListOfCertifiedWalletsURL	ISO-8859-1 Byte mode QR code	Facultatif
WalletSolutionInfoPageURL	URL de la page d'information de la solution de portefeuille certifiée de ListOfCertifiedWalletsURL complétée par un '?' et l'identifiant WalletSolutionID de la solution de portefeuille.	URL	Obligatoire
WalletSolutionInfoPageQRCode	Code QR contenant les informations de WalletSolutionInfoPageURL	ISO-8859-1 Byte mode QR code	Facultatif
WalletVerifierToolURL *	URL renvoyant au point de terminaison de l'outil de vérification du portefeuille */.well-known/openid-credential-issuer* utilisé pour extraire les métadonnées du fournisseur d'attestation.	URL	Facultatif

([1]) Règlement d'exécution (UE) 2025/849 de la Commission du 6 mai 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne la communication à la Commission et au groupe de coopération d'informations destinées à la liste des portefeuilles européens d'identité numérique certifiés (JO L, 2025/849, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj).»

ANNEXE X

L'annexe II du règlement d'exécution (UE) 2024/2980 est modifiée comme suit:

1) à l'annexe II, section 1, le point 1), i), est remplacé par le texte suivant:

«i) un ou plusieurs certificats conformes à la norme ETSI EN 319 412-2 V2.4.1 (2025-06) ou à la norme ETSI EN 319 412-3 V1.3.1 (2023-09) qui peuvent être utilisés pour vérifier la signature ou le cachet créés par le bureau d'enregistrement concernant les informations du registre, et pour lesquels les données d'identité certifiées comprennent le nom du bureau d'enregistrement et, le cas échéant, son numéro d'immatriculation, comme prévu respectivement aux points c) et d);»;

2) à l'annexe II, section 2, le point 1), h), est remplacé par le texte suivant:

«h) un ou plusieurs certificats conformes à la norme ETSI EN 319 412-2 V2.4.1 (2025-06) ou à la norme ETSI EN 319 412-3 V1.3.1 (2023-09) qui peuvent être utilisés pour authentifier et valider les attestations d'unité de portefeuille délivrées par le fournisseur de portefeuille, et pour lesquels les données d'identité certifiées comprennent le nom du fournisseur de portefeuille et, le cas échéant, son numéro d'immatriculation, comme prévu respectivement aux points a) et b);»;

3) à l'annexe II, section 3, le point 1), h), est remplacé par le texte suivant:

«h) un ou plusieurs certificats conformes à la norme ETSI EN 319 412-2 V2.4.1 (2025-06) ou à la norme ETSI EN 319 412-3 V1.3.1 (2023-09) qui peuvent être utilisés pour vérifier la signature ou le cachet créés par le fournisseur de données d'identification personnelle concernant les données d'identification personnelle qu'il fournit, et pour lesquels les données d'identité certifiées comprennent le nom du fournisseur de données d'identification personnelle et, le cas échéant, son numéro d'immatriculation, comme prévu respectivement aux points a) et b).»;

4) à l'annexe II, section 4, le point 1), g), est remplacé par le texte suivant:

«g) un ou plusieurs certificats conformes à la norme ETSI EN 319 412-2 V2.4.1 (2025-06) ou à la norme ETSI EN 319 412-3 V1.3.1 (2023-09) qui peuvent être utilisés pour vérifier la signature ou le cachet créés par le fournisseur de certificats d'accès de partie utilisatrice de portefeuille sur les certificats d'accès qu'il fournit aux parties utilisatrices de portefeuille avec, le cas échéant, les informations nécessaires pour distinguer les certificats d'accès de partie utilisatrice de portefeuille d'autres certificats.»;

5) à l'annexe II, la section 5 suivante est ajoutée:

«5. Notifications d'informations concernant les fournisseurs de certificats d'enregistrement de partie utilisatrice de portefeuille

1. Les États membres transmettent à la Commission les informations suivantes concernant les fournisseurs de certificats d'enregistrement de partie utilisatrice de portefeuille:

a) le nom du fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille;

b) le cas échéant, le numéro d'immatriculation du fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille;

c) l'État membre dans lequel le fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille est établi;

d) l'adresse électronique et le numéro de téléphone auxquels le fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille est joignable pour des questions relatives aux certificats d'enregistrement qu'il fournit aux parties utilisatrices de portefeuille;

e) le cas échéant, l'adresse URL de la page web du fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille contenant des informations supplémentaires sur le fournisseur et les certificats d'enregistrement qu'il fournit aux parties utilisatrices de portefeuille;

f) l'adresse URL de la page web où figurent les politiques et les conditions applicables à la fourniture et à l'utilisation des certificats d'enregistrement qu'il fournit aux parties utilisatrices de portefeuille;

g) un ou plusieurs certificats conformes à la norme ETSI EN 319 412-2 V2.4.1 (2025-06) ou à la norme ETSI EN 319 412-3 V1.3.1 (2023-09) qui peuvent être utilisés pour vérifier la signature ou le cachet créés par le fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille sur les certificats d'enregistrement qu'il fournit aux parties utilisatrices de portefeuille avec, le cas échéant, les informations nécessaires pour distinguer les certificats d'enregistrement de partie utilisatrice de portefeuille d'autres certificats.

2. Les informations visées au point 1 sont transmises pour chaque fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille.».

ANNEXE XI

«ANNEXE I

Protocoles et interfaces visés à l'article 4

La spécification technique ETSI TS 119 472-3 V1.1.1 (2026-03) s'applique moyennant les adaptations suivantes:

1) 4.1. General requirements

— GEN-REQ-4.1-05: vide.

— *REMARQUE:* vide.

2) 4.2.3. Provision of registration certificates of PID/EAA Provider to EUDI Wallet

— ISS-MDATA-REG_CERT-4.2.3-04: L'un des éléments du paramètre de tableau issuer_info contient le certificat d'enregistrement du fournisseur de PID/EAA.

— ISS-MDATA-REG_CERT-4.2.3-07: vide.

— ISS-MDATA-REG_CERT-4.2.3-08: vide.

— ISS-MDATA-REG_CERT-4.2.3-09: vide.

— ISS-MDATA-REG_CERT-4.2.3-10: vide.

— ISS-MDATA-REG_CERT-4.2.3-11: vide.

— ISS-MDATA-REG_CERT-4.2.3-12: vide.

— ISS-MDATA-REG_CERT-4.2.3-13: vide.

3) 4.2.4.2 ARF pre-defined PID/EAA reuse policy

— ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: lorsque le membre id a la valeur 'arf_annex_ii' et que le tableau associé à l'étiquette 'details' contient la valeur 'once_only' ou la valeur 'per relying-party', l'objet JSON qui contient ce tableau associé à l'étiquette 'details' doit aussi contenir un numéro JSON associé à l'étiquette 'reissue_trigger_unused'.

4) L'annexe A ne s'applique pas.».

ANNEXE XII

«ANNEXE II

Spécifications techniques visées à l'article 5

Les spécifications techniques de l'annexe C de la norme ISO/IEC 18013-7: 2025 s'appliquent.

Les spécifications techniques des paragraphes 4.1, 4.2, 5 et 6 de la norme ETSI TS 119 472-2 V1.2.1 (2026-03) s'appliquent moyennant les adaptations suivantes, notamment l'insertion d'un nouveau paragraphe 4.3:

1) 1. Champ d'application

— Le présent document spécifie deux profils de protocoles permettant aux parties utilisatrices (RP) de demander des EAAP ou des données d'identification personnelle (PID) au portefeuille européen d'identité numérique, et au portefeuille européen d'identité numérique d'envoyer à la RP les EAAP/PID demandées. Chacun de ces profils prend en charge deux mécanismes de transmission, à savoir: avec médiation d'API et sans médiation d'API, comme suit:

a) Un profil se fonde sur:

— ISO/IEC 18013-5 [10] pour le mécanisme de transmission sans médiation d'API uniquement, et

— sur l'annexe C de la norme ISO/IEC 18013-7 [16] pour le mécanisme de transmission avec médiation d'API.

Ce profil est appelé profil ISO/IEC-mdoc et il est défini au paragraphe 5 du présent document.

b) Un profil se fonde sur:

OpenID4VC-HAIP [11] à la fois pour les mécanismes de transmission avec médiation d'API et sans médiation d'API, comme suit:

— les sections 5, 5.1, 5.3, 7 et 8 de [11] pour la transmission via Redirects ou un mécanisme de transmission sans médiation d'API, et

— les sections 5, 5.2, 5.3, 7 et 8 de [11] pour la transmission par un mécanisme de transmission avec médiation d'API.

Ce profil est appelé profil OpenID4VC-HAIP et il est défini au paragraphe 6 du présent document.

2) 2.1. Références normatives

— [15] ISO 639: 'Language code'

— [16] ISO/IEC 18013-7: 2025 'Personal identification – ISO – compliant driving licence – Part 7: Mobile driving licence (mDL) add-on functions' (Identification des personnes – Permis de conduire conforme à l'ISO – Partie 7: Fonctionnalités supplémentaires pour permis de conduire sur téléphone mobile).

3) 4.1. EAAP implementation based on SD-JWT VC

— EAAP-SD-JWT VC-04: vide.

4) 4.2. EAAP implementation based on ISO/IEC-mdoc

— EAAP-ISO/IEC-mdoc-01: vide.

— *Remarque 2:* vide.

— EAAP-ISO/IEC-mdoc-02: vide.

5) 4.3. EAAP implementation with mediating API

— EAAP-API-GEN-01: le portefeuille européen d'identité numérique prend en charge une API de médiation qui accepte les deux protocoles définis au paragraphe 5.2 du [11] et à l'annexe C du [16].

— *REMARQUE:* lorsque l'appareil sur lequel le portefeuille européen d'identité numérique est installé ne prend pas en charge les deux protocoles, cette exigence ne peut pas être satisfaite, ce qui entraîne une non-conformité due au fait que les systèmes d'exploitation et navigateurs sous-jacents ne mettent pas en œuvre les caractéristiques d'interopérabilité nécessaires.

— EAAP-API-GEN-02: le portefeuille européen d'identité numérique prend en charge une API de médiation au moins pour les types de PID et d'EAA enregistrés dans le catalogue de programmes tel que défini dans le règlement d'exécution (UE) 2025/1569, et au moins pour tous les formats définis à l'annexe II du règlement d'exécution (UE) 2024/2979.

— *REMARQUE 1:* lorsque le système d'exploitation, le navigateur ou les API de médiation sous-jacents, ou toute autre couche technique échappant au contrôle du portefeuille européen d'identité numérique restreint, filtre, présélectionne ou limite d'une autre manière les formats de justificatifs d'identité, ainsi que les types de PID et d'EAA enregistrés dans le catalogue des de programmes, cette exigence ne peut être satisfaite. Lorsqu'une telle restriction empêche le portefeuille européen d'identité numérique de prendre en charge un type ou un format de justificatif d'identité enregistré, la non-conformité qui en résulte est imputable au fait que ces systèmes d'exploitation, navigateurs, API de médiation ou autres couches techniques pertinentes sous-jacents ne fournissent pas les caractéristiques d'interopérabilité nécessaires.

6) 4.4. Wallet-relying party validation and overasking checks

— WRP-VALIDATION-01: le portefeuille européen d'identité numérique doit valider le certificat d'enregistrement de partie utilisatrice de portefeuille reçu dans la demande avant de présenter toute PID ou attestation électronique d'attributs demandée à l'utilisateur de portefeuille pour approbation.

— WRP-VALIDATION-02: en cas d'échec de la validation du certificat d'enregistrement de partie utilisatrice de portefeuille, y compris lorsque le certificat a expiré, a été révoqué, n'a pas été délivré par un fournisseur de confiance valide de certificats d'enregistrement de partie utilisatrice de portefeuille, n'a pas été correctement formé ou ne peut pas être vérifié par des moyens cryptographiques, le portefeuille européen d'identité numérique doit avertir l'utilisateur de portefeuille que la partie utilisatrice de portefeuille n'a pas pu être validée et ne doit pas indiquer que la validation de la demande a réussi. L'utilisateur de portefeuille doit approuver explicitement la demande de la partie utilisatrice. Ni l'absence de réponse ni des cases cochées par défaut n'ont valeur d'approbation explicite.

— WRP-VALIDATION-03: le fournisseur de portefeuille doit déterminer, sur la base de son analyse des risques et de sa politique de sécurité, si et dans quelles conditions l'utilisateur de portefeuille peut contourner des contrôles de validation spécifiques ayant échoué.

— WRP-OVERASKING-01: le portefeuille européen d'identité numérique doit comparer les attestations et attributs demandés par la partie utilisatrice de portefeuille avec les attestations et attributs enregistrés dans le certificat d'enregistrement de partie utilisatrice de portefeuille.

— WRP-OVERASKING-02: lorsque la partie utilisatrice de portefeuille demande des PID ou des attestations électroniques d'attributs ou des revendications qui ne sont pas couvertes par le certificat d'enregistrement de partie utilisatrice de portefeuille, le portefeuille européen d'identité numérique doit émettre un avertissement clair à l'intention de l'utilisateur de portefeuille avant toute divulgation. L'avertissement doit indiquer que la partie utilisatrice de portefeuille demande davantage d'informations que celles qui ont été enregistrées. L'utilisateur de portefeuille doit approuver explicitement la demande de la partie utilisatrice. Ni l'absence de réponse ni des cases cochées par défaut n'ont valeur d'approbation explicite.

— WRP-OVERASKING-03: le fournisseur de portefeuille doit déterminer, sur la base de son analyse des risques, de sa politique de sécurité et du droit applicable, si l'utilisateur de portefeuille peut continuer malgré cet avertissement, si seul le sous-ensemble de données demandées couvert par le certificat d'enregistrement peut être divulgué ou si la demande doit être rejetée.

7) 5.1. Introduction

— Le paragraphe 5 et ses sous-paragraphes définissent un profil pour un protocole permettant à une RP de demander des EAAP ou des PID au portefeuille européen d'identité numérique, et à ce portefeuille d'envoyer les EAAP/PID demandées à la RP au moyen soit d'un mécanisme de transmission sans médiation d'API, fondé sur la norme ISO/IEC 18013-5 [10], soit d'un mécanisme de transmission avec médiation d'API fondé sur l'annexe C de la norme ISO/IEC 18013-7 [16] pour le transfert des structures de données définies dans la norme ISO/IEC 18013-5 [10] convenablement encapsulées.

— Le reste du paragraphe 5 est organisé comme suit:

  — le paragraphe 5.2 définit les exigences relatives à la prise en charge du profil et des mécanismes de transmission par les RP et le portefeuille européen d'identité numérique;

  — le paragraphe 5.3 précise les exigences spécifiquement applicables au mécanisme de transmission sans médiation d'API;

  — le paragraphe 5.4 et ses sous-paragraphes précisent les exigences spécifiquement applicables au mécanisme de transmission avec médiation d'API.

8) 5.2. Requirements on EUDI Wallet and RP support

— ISO/IEC 18013-SUPPORT-01: les unités de portefeuille, les fournisseurs de PID, les fournisseurs d'attestations, les fournisseurs de portefeuille et les parties utilisatrices ne prennent pas en charge la récupération sur serveur telle que spécifiée dans la norme ISO/IEC 18013-5 [10] pour demander et présenter des PID ou des attributs d'attestations.

— ISO/IEC 18013-SUPPORT-02: le portefeuille européen d'identité numérique doit être conforme aux exigences définies aux paragraphes 5.3 et 5.4 du présent document.

— ISO/IEC 18013-SUPPORT-04: il convient qu'une partie utilisatrice mette en œuvre le profil défini au paragraphe 5.4 du présent document.

9) 5.3.2 ISO/IEC-mdoc EAAP Request contents

— ISO/IEC 18013-5-REQ-04: les demandes envoyées par l'appareil au portefeuille européen d'identité numérique doivent contenir la paire clé-valeur 'requestInfo' spécifiée au paragraphe 8.3.2.1.2.1 de [10]. La valeur de cette paire doit être du type RequestInfo.

— ISO/IEC 18013-5-REQ-05: le type RequestInfo doit correspondre à la définition CDDL ci-dessous:

```
RequestInfo = {

    'euWrprc': bstr ; contient un certificat d'enregistrement (voir les exigences ci-dessous)

}
```

— ISO/IEC 18013-5-REQ-06: le membre requestInfo mentionné doit comporter un membre muni de l'étiquette 'euWrprc'.

— ISO/IEC 18013-5-REQ-07: la valeur de la paire 'euWrprc' doit être un certificat d'enregistrement encodé au format CBOR.

— ISO/IEC 18013-5-REQ-08: vide.

— *REMARQUE 3:* vide.

— ISO/IEC 18013-5-REQ-09: vide.

— ISO/IEC 18013-5-REQ-10: vide.

— ISO/IEC 18013-5-REQ-11: vide.

10) 5.3.3. ISO/IEC-mdoc EAAP Response profile

— Le présent paragraphe définit les exigences applicables au type de message DeviceResponse, commun aux deux types de mécanismes de transmission (avec et sans médiation d'API).

— *REMARQUE 1:* lorsqu'un mécanisme sans médiation d'API fondé sur la norme ISO/IEC 18013-5 [10] est utilisé, une réponse EAAP est exactement une instance de DeviceResponse telle que décrite dans le présent paragraphe. Lorsqu'un mécanisme avec médiation d'API fondé sur l'annexe C de la norme ISO/IEC 18013-7 [16] est utilisé, l'instance de DeviceRequest est encapsulée comme spécifié à l'annexe C du [16].

— ISO/IEC 18013-5-RESP-02: le fournisseur de données d'identification personnelle et d'attestations électroniques d'attributs n'inclut aucun élément de données de la table associative KeyAuthorizations de l'objet de sécurité mobile des données d'identification personnelle et des attestations électroniques d'attributs qu'il délivre, à l'exception des éléments de données qui sont fournis par la partie utilisatrice de portefeuille dans les données transactionnelles de la demande mdoc, qui doit être signée ou cachetée par l'unité de portefeuille à l'aide de la clé privée des données d'identification personnelle ou des attestations électroniques d'attributs.

— *REMARQUE 2:* par conséquent, les unités de portefeuille ne peuvent pas présenter aux parties utilisatrices de portefeuille d'éléments de données signés par le dispositif, à l'exception des données que la partie utilisatrice de portefeuille a fournies, par exemple pour une authentification sécurisée de l'utilisateur.

— *REMARQUE 3:* la norme ISO/IEC 18013-5: 2021 ne précise pas comment les parties utilisatrices de portefeuille peuvent inclure des données transactionnelles dans une demande mdoc. L'inclusion de données transactionnelles dans une demande mdoc nécessite des spécifications techniques supplémentaires.

— ISO/IEC 18013-5-RESP-03: les fournisseurs de données d'identification personnelle n'autorisent pas la clé privée des données d'identification personnelle à signer les éléments de données qui sont fournis par la partie utilisatrice de portefeuille dans les données transactionnelles figurant dans la demande mdoc.

11) 5.4. Requirements for API mediated mechanism

5.4.1. ISO/IEC 18013-7-related requirements

Le présent paragraphe définit les exigences applicables au mécanisme de transmission avec médiation d'API en rapport avec les exigences définies à l'annexe C du [16].

— ISO/IEC 18013-7-API-01: le profil prenant en charge les présentations avec médiation d'API doit être conforme aux exigences de l'annexe C de la norme ISO/IEC 18013-7 [16] telles que précisées dans les paragraphes 5.3 et 5.4 du présent document.

— ISO/IEC 18013-7-API-02: toutes les exigences obligatoires définies à l'annexe C du [16] sont applicables, telles que précisées dans les paragraphes 5.3 et 5.4 du présent document.

— ISO/IEC 18013-7-API-03: toutes les exigences facultatives définies à l'annexe C du [16] doivent rester facultatives, sauf indication contraire dans le présent document.

12) 5.4.2. Additional requirements

— Le présent paragraphe spécifie des exigences supplémentaires pour le mécanisme de transmission avec médiation d'API.

— ISO/IEC 18013-ADD-API-01: le portefeuille européen d'identité numérique doit divulguer par défaut la présence de tous les types d'attestations électroniques d'attributs stockés à l'API de médiation qui fonctionne conformément à l'annexe C du [16], mais il ne doit pas divulguer les attributs et leurs valeurs dans ces attestations électroniques d'attributs.

— *REMARQUE 1:* la restriction concernant la valeur des attributs s'applique même si cette divulgation aurait pour effet d'améliorer les services fournis par le système d'exploitation au portefeuille, par exemple la sélection de l'attestation dans le cadre de l'API assurant la médiation.

— Certaines considérations relatives aux systèmes d'exploitation et aux navigateurs échappent au contrôle des responsables de la mise en œuvre et peuvent être prises en compte comme indiqué dans les remarques 2 à 4 suivantes:

— *REMARQUE 2:* une demande de présentation émanant d'une partie utilisatrice prenant en charge l'annexe C du [16] peut être traitée par le navigateur et/ou le système d'exploitation pour rechercher des EAA disponibles, pour prévenir une fraude ciblant l'utilisateur ou à des fins de dépannage.

— *REMARQUE 3:* une demande de présentation émanant d'une partie utilisatrice prenant en charge l'annexe C du [16] est censée être traitée par le navigateur et/ou le système d'exploitation pour la sécurité de l'utilisateur.

— *REMARQUE 4:* une demande de présentation émanant d'une partie utilisatrice prenant en charge l'annexe C de [16] ne devrait pas être traitée par le navigateur et/ou le système d'exploitation à des fins d'analyse de marché (y compris à titre secondaire) ou à des fins internes du navigateur et/ou du système d'exploitation.

— ISO/IEC 18013-ADD-API-02: lorsqu'un portefeuille européen d'identité numérique supprime, à la demande de l'utilisateur, des PID ou une EAA précédemment divulguées à l'API assurant la médiation qui fonctionne conformément à l'annexe C du [16], le portefeuille indique à l'API assurant la médiation qu'il ne stocke plus ces PID ou cette EAA.

— ISO/IEC 18013-ADD-API-03: si l'utilisateur désinstalle son portefeuille européen d'identité numérique, le portefeuille divulgue le fait qu'il ne stocke plus aucun des PID ou EAA précédemment divulgués à l'API de médiation qui fonctionne conformément à l'annexe C du [16].

— ISO/IEC 18013-ADD-API-04: le portefeuille européen d'identité numérique comporte un paramètre utilisateur global permettant de désactiver la divulgation des EAA stockées via une API de médiation qui fonctionne conformément aux spécifications de la norme ISO/IEC 18013-ADD-API-01. Lorsque ce paramètre est désactivé, le portefeuille ne fait pas d'annonce ou ne répond pas aux demandes de présentation ou d'émission transmises par l'API.

— ISO/IEC 18013-ADD-API-05: les portefeuilles européens d'identité numérique vérifient dans les flux multi-appareils, à l'aide de l'API de médiation, que l'appareil qui interagit se trouve à proximité physique immédiate du portefeuille européen d'identité numérique, au moyen d'un canal de communication local sécurisé, direct et nécessitant une action de l'utilisateur, tel qu'une technologie de communication sans fil à courte portée, pour effectuer la vérification de proximité physique.

— *REMARQUE:* le protocole CTAP 2.3 permet d'utiliser le BLE pour effectuer la vérification de proximité physique immédiate et, lorsqu'il est mis en œuvre par les deux appareils, permet également de transporter les données d'un appareil à l'autre au moyen de technologies de transmission à courte portée. Les systèmes d'exploitation, navigateurs, API de médiation sous-jacents ou toute autre couche technique échappant au contrôle du portefeuille européen d'identité numérique devraient utiliser, pour réaliser tant la vérification de proximité physique que le transfert de données entre les deux appareils, un canal de communication local comme prévu par le CTAP 2.3 plutôt que de recourir aux services de transport hybride CTAP.

13) 6.2 Requirements on EUDI Wallet and RP support

— OIDFVP-HAIP-SUPPORT-02: le portefeuille européen d'identité numérique doit être conforme aux exigences définies au paragraphe 6.5 de la présente annexe.

— OIDFVP-HAIP-SUPPORT-03: le portefeuille européen d'identité numérique ne devrait pas prendre en charge le mécanisme fondé sur les redirections spécifié au paragraphe 6.4 pour les flux de présentation multi-appareils.

— *REMARQUE 3:* ce mécanisme est vulnérable aux attaques, notamment par fixation des sessions. Il appartient aux parties utilisatrices d'atténuer ces attaques. La mise en œuvre de ce mécanisme ne devrait pas entraîner de non-conformité.

— OIDFVP-HAIP-SUPPORT-05: une partie utilisatrice doit être conforme aux exigences définies au paragraphe 6.5 de la présente annexe.

— *REMARQUE 5:* vide.

14) 6.3.1. General requirements

— OIDFVP-HAIP-GEN-01: toutes les exigences obligatoires énoncées aux paragraphes 5, 5.3, 7 et 8 de HAIP [11] s'appliquent.

— *REMARQUE 1:* "Section 5 de HAIP [11]" renvoie uniquement aux exigences énoncées directement sous l'intitulé "Section 5". Cela n'inclut pas les sections 5.1, 5.2 et 5.3.

— OIDFVP-HAIP-GEN-03: si la présente annexe modifie une exigence dans OpenID4VC-HAIP [11], l'exigence modifiée spécifiée par la présente annexe prévaut.

— *REMARQUE 2:* cela permettrait, par exemple, de rendre obligatoire une exigence facultative de OpenID4VC-HAIP [11] ou d'étendre des exigences obligatoires.

— OIDFVP-HAIP-GEN-04: lorsque le format de l'attestation demandée est conforme à [10], les parties utilisatrices et les portefeuilles européens d'identité numérique doivent être conformes au profil 'ISO mdocs' figurant à la section 6 de [11].

— *REMARQUE 3:* éclaircissement: le profil 'ISO mdocs' dans HAIP implique que les parties utilisatrices et les portefeuilles européens d'identité numérique doivent être conformes aux exigences applicables figurant à la section [7] de l'annexe B.2.

— OIDFVP-HAIP-GEN-05: lorsque le format de l'attestation demandée est conforme à [2], les parties utilisatrices et les portefeuilles européens d'identité numérique doivent être conformes au profil 'IETF SD-JWT VCs' figurant à la section 6 de [11].

— *REMARQUE 4:* éclaircissement: le profil 'IETF SD-JWT VCs' implique que les parties utilisatrices et les portefeuilles européens d'identité numérique doivent être conformes aux exigences figurant à la section [7] de l'annexe B.3, ainsi qu'aux exigences figurant à la section 6.1 de [11].

15) 6.3.2.1 General requirements

— OIDFVP-HAIP-COMMON-REQ-01: vide.

16) 6.3.2.2 Requirements for the Request Object

— OIDFVP-HAIP-COMMON-REQ-RO-02: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-03: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-04: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-05: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-06: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-07: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-08: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-09: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-10: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-11: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-12: vide.

— *Remarque 2:* vide.

— OIDFVP-HAIP-COMMON-REQ-RO-13: l'un des éléments du paramètre verifier_info comprend le certificat d'enregistrement.

— OIDFVP-HAIP-COMMON-REQ-RO-23: le certificat d'entité finale mentionné dans la section 5.9.3 d'OpenID4VP, à utiliser avec le x509_hash Client Identifier Prefix est un certificat d'accès de RP tel que spécifié dans ETSI TS 119 475 [14].

17) 6.3.3 Authorization Response (EAAP response) profile

— OIDFVP-HAIP-COMMON-RESP-01: vide.

18) 6.4.1 General requirements

— OIDFVP-HAIP-REDIRECTS-04: vide.

— *REMARQUE:* vide.

19) 6.5.2 General requirements

— OIDFVP-HAIP-ADD-API-01: le portefeuille européen d'identité numérique doit divulguer par défaut la présence de tous les types d'EAA stockées à l'API assurant la médiation qui fonctionne conformément au paragraphe 5.2 de [11], mais il ne doit pas divulguer les attributs et leurs valeurs dans ces EAA.

— OIDFVP-HAIP-ADD-API-04: si le portefeuille européen d'identité numérique prend en charge une API de médiation qui fonctionne comme indiqué dans OIDFVP-HAIP-ADD-API-01, il doit comporter un paramètre utilisateur global permettant de désactiver la divulgation des EAA stockées par l'intermédiaire de l'API de médiation. Lorsque ce paramètre est configuré en divulgation désactivée, le portefeuille européen d'identité numérique devrait ensuite permettre à l'utilisateur de sélectionner individuellement les attestations à divulguer à l'API de médiation.

— OIDFVP-HAIP-ADD-API-05: les portefeuilles européens d'identité numérique doivent utiliser, dans les flux multi-appareils, l'API de médiation pour vérifier que l'appareil qui interagit se trouve à proximité physique immédiate du portefeuille européen d'identité numérique, au moyen d'un canal de communication local sécurisé, direct et nécessitant une action de l'utilisateur, tel qu'une technologie de communication sans fil à courte portée, pour effectuer la vérification de proximité physique.

— *REMARQUE 5:* le protocole CTAP 2.3 permet d'utiliser le BLE pour effectuer la vérification de proximité physique immédiate et, lorsqu'il est mis en œuvre par les deux appareils, permet également de transporter les données d'un appareil à l'autre au moyen de technologies de transmission à courte portée. Les systèmes d'exploitation, navigateurs, API de médiation sous-jacents ou toute autre couche technique échappant au contrôle du portefeuille européen d'identité numérique devraient utiliser, pour réaliser tant la vérification de proximité physique que le transfert de données entre les deux appareils, un canal de communication local comme prévu par le CTAP 2.3 plutôt que de recourir aux services de transport hybride CTAP.

20) 6.5.3 Specific requirements when requesting ISO/IEC 18013-5 EAAP

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: toutes les exigences énoncées dans le présent document applicables aux structures Device Request et Device Response précisées dans ISO/IEC 18013-5 sont également applicables lorsque le portefeuille européen d'identité numérique reçoit une demande de présentation ISO/IEC mdoc via un mécanisme transmis par API figurant dans le paragraphe C.1 de [16].»