Journal officiel
de l'Union européenne

FR
Série L

2026/798

8.4.2026

RÈGLEMENT D'EXÉCUTION (UE) 2026/798 DE LA COMMISSION

du 7 avril 2026

portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne les normes de référence et les spécifications applicables à l'enrôlement à distance des utilisateurs pour les portefeuilles européens d'identité numérique par des moyens d'identification électronique conformes au niveau de garantie substantiel combinés avec des procédures d'enrôlement à distance supplémentaires lorsque la combinaison répond aux exigences du niveau de garantie élevé

LA COMMISSION 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 24,

considérant ce qui suit:

(1) L'enrôlement des utilisateurs pour les portefeuilles européens d'identité numérique (ci-après les «portefeuilles») est une étape essentielle dans la vérification de l'identité des utilisateurs de portefeuille et l'établissement du lien entre les données d'identification personnelle des utilisateurs et leur portefeuille et le dispositif utilisateur sur lequel les unités de portefeuille sont installées.

(2) Afin de favoriser un niveau élevé de confiance et de sécurité ainsi qu'une approche harmonisée dans l'ensemble des États membres pour l'enrôlement des utilisateurs de portefeuille par des procédures d'enrôlement à distance combinées avec les moyens d'identification électronique conformes au niveau de garantie substantiel, le présent acte d'exécution établit des spécifications et des procédures afin de faciliter l'enrôlement des utilisateurs pour le portefeuille européen d'identité numérique par des moyens d'identification électronique conformes au niveau de garantie substantiel combinés avec des procédures d'enrôlement à distance supplémentaires qui, conjointement, répondent aux exigences du niveau de garantie élevé.

(3) Ces normes devraient tenir compte des pratiques établies et être largement reconnues dans les secteurs concernés. Elles devraient faire l'objet d'adaptations visant à y inclure des exigences qui garantissent la sécurité et la fiabilité de l'enrôlement des utilisateurs.

(4) Le règlement d'exécution (UE) 2015/1502 de la Commission ([2]) dispose que, lorsque des moyens d'identification électronique sont délivrés au niveau de garantie élevé, et en tenant compte des risques d'une modification des données d'identification personnelle, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité. Par conséquent, en pareil cas, les États membres devraient se servir de moyens d'identification électronique délivrés au niveau de garantie élevé pour les appliquer également au processus d'enrôlement aux fins du présent règlement.

(5) Lorsque les États membres enrôlent des utilisateurs pour des portefeuilles par un moyen d'identification électronique qui n'a pas été notifié à la Commission, le niveau de garantie de ce moyen devrait être confirmé par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 du Parlement européen et du Conseil ([3]) ou par un organisme équivalent et il devrait être démontré que les résultats de cette procédure de délivrance antérieure d'un moyen d'identification électronique restent valables.

([1]) JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

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

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

(6) Bien que l'annexe énonce les exigences à remplir pour atteindre un niveau spécifique de preuve d'identité, l'équivalence n'a pas été établie en ce qui concerne les niveaux de garantie définis à l'article 8 du règlement (UE) nº 910/2014. Par conséquent, les exigences énoncées dans l'annexe devraient être considérées comme mettant en œuvre celles du règlement d'exécution (UE) 2015/1502 et devant être remplies par le fournisseur de données d'identification personnelle ou une entité fournissant des services de preuve d'identité pour le compte de ce fournisseur.

(7) La Commission évalue régulièrement les nouvelles technologies, pratiques et spécifications techniques. Conformément au considérant 75 du règlement (UE) 2024/1183 du Parlement européen et du Conseil ([4]), la Commission devrait réexaminer et, si besoin est, mettre à jour le présent règlement d'exécution, afin de le maintenir en adéquation avec les évolutions générales et les nouvelles technologies, normes ou spécifications techniques et de suivre les meilleures pratiques sur le marché intérieur, en particulier quant à l'enrôlement des utilisateurs pour le portefeuille.

(8) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([5]) ainsi que, le cas échéant, le règlement (UE) 2018/1725 du Parlement européen et du Conseil ([6]) et la directive 2002/58/CE du Parlement européen et du Conseil ([7]) s'appliquent aux activités de traitement de données à caractère personnel au titre du présent règlement.

(9) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 et a rendu son avis le 30 janvier 2026 ([8]).

(10) Le comité institué par l'article 48 du règlement (UE) nº 910/2014 n'a pas émis d'avis dans le délai fixé par sa présidence,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Les normes de référence et les spécifications mentionnées à l'article 5 *bis*, paragraphe 24, du règlement (UE) nº 910/2014 figurent à l'annexe du présent règlement.

([4]) Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique (JO L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([5]) 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).

([6]) 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).

([7]) 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]) EDPS Formal comments on the draft Commission Implementing Regulation as regards onboarding of users to the European Digital Identity Wallets.

Article 2

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 7 avril 2026.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE

LISTE DES NORMES DE RÉFÉRENCE ET SPÉCIFICATIONS

La conformité est évaluée au regard des clauses de la norme ETSI TS 119 461 V2.1.1 (2025-02) énumérées à la section 1, sous réserve des adaptations énumérées à la section 2.

Section 1 — Clauses applicables

—	5	Évaluation du risque opérationnel
—	6	Politiques et méthodes
—	7	Gestion et exploitation du service de preuve de l'identité
—	8	Exigences du service de preuve de l'identité
—	9.1	Introduction, conformité avec le présent document, exigences générales pour tous les cas d'utilisation
—	9.2.2	Cas d'utilisation à partir d'un document d'identité pour la preuve de l'identité à distance non automatisée
—	9.2.3	Cas d'utilisation à partir d'un document d'identité pour la preuve de l'identité à distance automatisée
—	9.2.4	Cas d'utilisation pour la preuve de l'identité par authentification à partir de moyens d'identification électronique
—	9.5	Cas d'utilisation pour une preuve d'identité supplémentaire visant à renforcer une identité prouvée au moyen d'une identification électronique à partir du niveau Baseline LoIP vers le niveau Extended LoIP.

Section 2 — Adaptations

1.	5	Évaluation du risque opérationnel
	—	OVR-5-01: Les exigences spécifiées dans l'ETSI EN 319 401 [1], clause 5, doivent s'appliquer.
	—	*Note 1*: Lorsque la preuve de l'identité est effectuée par le fournisseur de données d'identification personnelle lui-même, l'évaluation des risques du fournisseur de données d'identification personnelle peut couvrir la preuve de l'identité.
2.	6.1	Énoncé des pratiques du service de preuve d'identité
	—	OVR-6.1-02: Un IPSP identifie dans son énoncé des pratiques les cas d'utilisation pour lesquels la conformité avec le présent document est alléguée.
	—	*Note 1:* Lorsque la preuve de l'identité est effectuée par le fournisseur de données d'identification personnelle lui-même, l'énoncé des pratiques du service de preuve d'identité du fournisseur de données d'identification personnelle peut couvrir les informations relatives à la preuve d'identité et il n'est pas nécessaire d'établir d'énoncé des pratiques spécifique pour la preuve d'identité.
3.	7.9	Vulnérabilités et gestion des incidents
	—	OVR-7.9-02: Les obligations de déclaration conformément à la norme ETSI EN 319401 [1] REQ-7.9.2-02X et à la clause 7.9.3 doivent être remplies en fonction du contexte d'établissement de la preuve d'identité et des obligations du fournisseur de données d'identification personnelle dépendant du service de l'IPSP.
	—	Exemple: Les déclarations à l'autorité de contrôle chargée de la surveillance d'un fournisseur de portefeuilles européens d'identité numérique établi dans l'État membre qui a procédé à la désignation peuvent être effectuées en coopération entre l'IPSP et le fournisseur de données d'identification personnelle.

4. 7.10 Collecte d'éléments de preuve

— OVR-7.10-01: Les exigences spécifiées dans l'ETSI EN 319401 [1], clause 7.10, doivent s'appliquer.

— *Note 1:* Les exigences à long terme en matière de conservation des éléments de preuve peuvent être remplies par le fournisseur de données d'identification personnelle demandant la preuve d'identité plutôt que par l'IPSP lorsque les deux entités sont différentes.

— *Note 2:* Les exigences de la clause 8.5.2 du présent document s'appliquent.

5. 7.11 Gestion de la continuité des activités

— OVR-7.11-02: Les processus de gestion de crises conformément à la norme ETSI EN 319401 [1], REQ-7.11.3-01X doivent être tels que le requièrent le contexte d'établissement de la preuve d'identité et les obligations du fournisseur de données d'identification personnelle dépendant du service de l'IPSP.

6. 7.12 Arrêt d'activité et plans d'arrêt d'activité

— OVR-7.12-01: Les exigences spécifiées dans la norme ETSI EN 319401 [1], clause 7.12, à l'exclusion de REQ-7.12-11, doivent s'appliquer.

— *Note:* Lorsque l'IPSP et le fournisseur de données d'identification personnelle demandant la preuve d'identité sont des entités différentes, ils peuvent convenir d'une assistance mutuelle ou unilatérale pour l'établissement des plans d'arrêt d'activité.

7. 8.1 Initiation

— INI-8.1-05: En cas d'interruption ou d'échec du processus de preuve d'identité à distance, l'IPSP doit veiller à ce que des explications et des possibilités de solution suffisantes soient fournies aux personnes, en particulier dans le cadre de la preuve d'identité à distance automatisée. Les informations devraient permettre aux personnes concernées de contribuer efficacement à la résolution rapide du problème et, si nécessaire, d'exercer leurs droits (tels que le droit de rectification ou la possibilité de contester la décision) à l'encontre du responsable du traitement concerné.

8. 8.2.1 Exigences générales

— COL-8.2.1-08: L'IPSP doit mettre en œuvre des mesures visant à garantir le respect des exigences en matière de protection des données dès la conception et par défaut conformément à l'article 25 du règlement (UE) 2016/679 au cours du processus d'enrôlement, en particulier en ce qui concerne le traitement des données biométriques. Les mesures en question peuvent comprendre, selon le cas, des contrôles cryptographiques, des dispositifs et des mesures organisationnelles de nature à renforcer la protection de la vie privée. Ces mesures devraient limiter la collecte de données à ce qui est strictement nécessaire au traitement des données biométriques et de toute autre donnée à caractère personnel à recueillir auprès des sources d'identification physiques et numériques en vue de relier les données d'identification personnelle de l'utilisateur à son portefeuille et à l'appareil de l'utilisateur sur lequel l'unité de portefeuille est installée.

9. 8.2.4 Utilisation de moyens d'identification électronique existants à titre d'élément de preuve

— [CONDITIONNEL] COL-8.2.4-02X: Si le niveau Baseline LoIP est visé, le moyen d'identification électronique doit avoir été notifié au moins au niveau de garantie substantiel d'eIDAS ou son niveau de garantie doit avoir été confirmé par un organisme d'évaluation de la conformité accrédité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou par un organisme équivalent et, si toutes les exigences applicables sont remplies, l'évaluation doit donner lieu à un certificat de conformité fondé sur un audit de certification. Ce processus formel de certification repose sur un processus d'évaluation de la sécurité qui fait référence aux niveaux de garantie définis pour les moyens d'identification électronique notifiés ou pour les portefeuilles européens d'identité numérique certifiés au titre du règlement (UE) nº 910/2014 [i.25].

— COL-8.2.4-02A: néant.

10. 8.3.1 Exigences générales

— VAL-8.3.1-11X: Le processus de preuve de l'identité vérifie que les éléments de preuve sont valables au moment de l'établissement de la preuve d'identité.

11. 8.3.3 Validation du document d'identité physique

— VAL-8.3.3-21: L'efficacité des mesures relatives à la conformité aux exigences VAL-8.3.3-05X, VAL-8.3.3-05A, VAL-8.3.3-05B, VAL-8.3.3-05C, VAL-8.3.3-07A et VAL-8.3.3-07X doit être confirmée par un organisme d'évaluation de la conformité accrédité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou un organisme équivalent.

— VAL-8.3.3-22: L'image faciale de référence du document d'identité physique est recueillie par communication en champ proche et le processus assure l'authentification passive ou active de la puce sur le document d'identité physique.

12. 9.1 Introduction, conformité avec le présent document, exigences générales pour tous les cas d'utilisation

— USE-9.1-01X: Pour être conforme au présent document, un processus de preuve d'identité doit être conforme au cas d'utilisation figurant à la clause 9.5 du présent document pour le niveau Extended LoIP.

— USE-9.1-03X: néant.

13. 9.2.3.4 Cas d'utilisation pour un fonctionnement automatisé

— USE-9.2.3.4-04: L'IPSP établit des valeurs cibles pour les FAR et les FRR, sur la base d'une analyse des risques et de sa procédure en matière de renseignement sur les menaces, en suivant la méthode établie dans le rapport de l'ENISA intitulé «Methodology for sectoral cybersecurity assessments» [i.28] ou une méthode équivalente, dans le cadre de processus entièrement automatisés de vérification de l'identité. Les valeurs cibles utilisées par l'IPSP sont égales ou inférieures à celles fixées pour les cas d'utilisation hybrides, lorsque ces derniers existent. L'IPSP maintient ces valeurs cibles pour les FAR et les FRR de manière cohérente, sur la base d'une analyse des risques et de sa procédure en matière de renseignement sur les menaces.

14. 9.5.1 Exigences générales

— Premier alinéa: Lorsque le demandeur est une personne physique, y compris une personne physique représentant une personne morale, que l'identité du demandeur a été prouvée au niveau Baseline LoIP par authentification à partir de moyens d'identification électronique et qu'un renforcement au niveau Extended LoIP est nécessaire, les exigences suivantes s'appliquent.

— USE-9.5.1-08: La preuve d'identité supplémentaire requise pour renforcer la fiabilité d'une identité ne s'applique qu'à l'identification électronique qui n'a pas été délivrée en recourant à une comparaison automatisée entre des images faciales pour le processus de délivrance initial.

15. 9.5.2 Cas d'utilisation pour le renforcement de la preuve d'identité au niveau Extended LoIP par l'établissement d'une preuve d'identité complète à partir d'un document d'identité

— USE-9.5.2-01: La preuve d'identité visant à passer du niveau Baseline LoIP au niveau Extended LoIP doit être conforme aux exigences applicables au niveau Extended LoIP dans l'un des cas d'utilisation décrits dans les clauses 9.2.2 ou 9.2.3 du présent document pour le niveau Extended LoIP.

16. 9.5.3 Cas d'utilisation pour le renforcement de la preuve d'identité au niveau Extended LoIP au moyen d'une image faciale de référence précédemment saisie

— USE-9.5.3-01: Un processus de preuve de l'identité satisfaisant aux exigences du niveau Extended LoIP dans l'un des cas d'utilisation décrits dans les clauses 9.2.2 ou 9.2.3 du présent document ou un processus de preuve de l'identité ayant fait l'objet d'un examen par les pairs ou ayant été certifié par un organisme d'évaluation de la conformité accrédité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou un organisme équivalent afin d'assurer un niveau de garantie élevé conformément au règlement (UE) nº 910/2014 [i.25] doit être utilisé pour saisir une image faciale de référence et lier les attributs d'identité nécessaires à cette image faciale de référence.