Journal officiel
de l'Union européenne

FR
Série L

2026/1735

22.7.2026

RÈGLEMENT D'EXÉCUTION (UE) 2026/1735 DE LA COMMISSION

du 15 juillet 2026

modifiant le règlement d'exécution (UE) 2025/1569 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 45 *quinquies*, paragraphe 5, son article 45 *sexies*, paragraphe 2, et son article 45 *septies*, paragraphes 6 et 7,

considérant ce qui suit:

(1) Afin de garantir le niveau d'harmonisation le plus élevé possible entre les États membres en matière de 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 l'adoption du règlement d'exécution (UE) 2025/1569 de la Commission ([3]), il convient à présent de modifier ledit règlement d'exécution afin de l'aligner sur les nouvelles normes et spécifications.

(2) Conformément aux objectifs du règlement (UE) nº 910/2014, un certain nombre de normes ont été sélectionnées pour satisfaire aux exigences applicables en matière de délivrance, de gestion et de vérification des attestations électroniques d'attributs. Ces normes devraient tenir compte des pratiques établies et être largement reconnues dans les secteurs concernés. Si nécessaire, ces normes devraient être adaptées ou complétées afin de garantir un niveau élevé de sécurité et d'intégrité des attestations électroniques d'attributs, tout en facilitant l'interopérabilité transfrontière et le bon fonctionnement du marché intérieur. Conformément à cet objectif, le présent règlement met à jour les exigences applicables à la délivrance et à la révocation des attestations électroniques d'attributs qualifiées et des attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte et introduit les exigences relatives à l'apposition d'une signature et d'un cachet sur les résultats de vérification par rapport aux sources authentiques.

(3) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([4]) et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([5]) s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du présent règlement.

([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) 2025/1569 de la Commission du 29 juillet 2025 portant modalités d'application du règlement (UE) nº 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).

([4]) 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).

([5]) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(4) 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 ([6]) et a rendu son avis le 17 avril 2026 ([7]).

(5) 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) 2025/1569

Le règlement d'exécution (UE) 2025/1569 est modifié comme suit:

1) À l'article 3, le paragraphe 2 est remplacé par le texte suivant:

«2. Lorsque les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte délivrent des attestations électroniques d'attributs qui sont couvertes par des programmes enregistrés dans le catalogue de programmes d'attestation d'attributs, ils se conforment aux exigences du programme d'attestation d'attributs correspondant. Les règles et procédures établies par les entités délivrant des attestations pour satisfaire aux exigences des programmes d'attestation d'attributs sont prises en compte dans l'évaluation de la conformité prévue par le règlement (UE) nº 910/2014.».

2) L'article 4 est modifié comme suit:

a) le paragraphe 1 est supprimé;

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

«3. Lorsque la période de validité des attestations fournies par les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte est supérieure à 24 heures, les fournisseurs de ces attestations les révoquent au moins dans les cas suivants:

a) à la demande de la personne à laquelle l'attestation électronique d'attributs a été délivrée ou, le cas échéant, de la personne à laquelle l'attestation se rapporte;

b) lorsque le fournisseur apprend que la sécurité ou la fiabilité 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 a été compromise;

c) dans d'autres situations, comme le requiert la législation de l'Union ou le droit national.»;

c) le paragraphe 4 est remplacé par le texte suivant:

«4. Les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte mettent en place des techniques de révocation et des méthodes de gestion des révocations qui garantissent la protection de la vie privée et empêchent l'associabilité et la traçabilité. Les techniques de révocation satisfont aux exigences énoncées à l'annexe II.».

([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]) EDPS Formal comments on the draft Commission Implementing Regulation as regards applicable standards and specifications for the registration of wallet-relying parties | (Commentaires formels du CEPD sur le projet de règlement d'exécution de la Commission en ce qui concerne les normes et spécifications applicables pour l'enregistrement des parties utilisatrices de portefeuille)Contrôleur européen de la protection des données.

3) L'article 9 est modifié comme suit:

a) le paragraphe 2 *bis* suivant est inséré après le paragraphe 2:

«2 *bis* Le mécanisme de vérification satisfait aux spécifications énoncées à l'annexe IV.»;

b) le paragraphe 4 est remplacé par le texte suivant:

«4. Le résultat de la vérification indique si l'attribut a été vérifié ou non et précise l'organisme du secteur public responsable de la source authentique ou, le cas échéant, l'organisme du secteur public désigné pour agir pour le compte de la source authentique ayant servi à la vérification de l'attribut.

Le résultat de la vérification est signé ou cacheté par l'organisme du secteur public responsable d'une source authentique, ou par l'intermédiaire désigné reconnu au niveau national, au moyen, au moins, d'une signature électronique avancée reposant sur un certificat qualifié de signature électronique ou d'un cachet électronique avancé reposant sur un certificat qualifié de cachet électronique, respectivement.».

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

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

6) Le texte figurant à l'annexe III du présent règlement est ajouté en tant qu'annexe IV.

Article 2

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 1er, paragraphe 3, est applicable à partir du 1er janvier 2027.

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 I*

Liste des normes de référence et des spécifications mentionnées à l'article 3

ETSI TS 119 471 V1.1.1 (2025-05) s'applique, moyennant les adaptations suivantes:

1) 2.1 Références normatives

[1] ETSI EN 319 401 V3.2.1 (2026-01): "Signatures électroniques et infrastructures de confiance; exigences de politique générale applicables des prestataires de services de confiance";

[2] 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);

[3] FIPS PUB 140-3 (2019) "Security Requirements for Cryptographic Modules";

[4] Règlement d'exécution (UE) 2024/482 de la Commission ([1]);

[5] Règlement d'exécution (UE) 2024/3144 de la Commission ([2]);

[6] ISO/IEC 15408:2022 (parties 1 à 5): "Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information".

2) 3.1 Termes

Le terme suivant est ajouté:

— Dispositif cryptographique sécurisé: dispositif qui contient la clé privée de l'utilisateur, protège cette clé contre toute compromission et exécute des fonctions de signature ou de déchiffrement pour le compte de l'utilisateur.

3) 4. Services de confiance de l'EAA

— La clause 4.2.2.2 «Vérification des attributs par rapport aux sources authentiques» ne s'applique pas.

— REQ-EAASP-4.2.2.3-02: Le prestataire de services d'attestation électronique d'attribut s'authentifie auprès de l'instance d'EUDIW en mettant en œuvre des mécanismes d'authentification mutuelle qui utilisent un certificat d'accès valide.

— REQ-EAASP-4.2.2.3-03: Le prestataire de services d'attestation électronique d'attribut valide l'unité d'EUDIW et vérifie si l'instance d'EUDIW est révoquée.

— La clause *4.3.2 'EUDIW Specific' ne s'applique pas.*

4) 6.1 Énoncé de pratique de l'EAAS:

— REQ-EAASP-6.1-02: Le prestataire de services d'attestation électronique d'attribut (EAASP) expose le mécanisme de révocation dans l'énoncé de pratique du service d'attestation électronique d'attribut (EAAS).

5) 6.3 Politique en matière de sécurité de l'information:

— REQ-EAASP-6.3-02: Le prestataire de services d'attestation électronique d'attribut établit des procédures pour informer l'organe de contrôle de toute modification apportée à la fourniture du service de confiance pour l'attestation électronique d'attributs et de l'intention de cesser ces activités, conformément aux exigences opérationnelles et aux dispositions législatives et réglementaires applicables, y compris conformément aux exigences des actes d'exécution adoptés en vertu de l'article 24, paragraphe 5, du règlement (UE) n° 910/2014. Le prestataire de services d'attestation électronique d'attribut adresse une notification à l'organe de contrôle au moins:

— un mois avant la mise en œuvre de toute modification;

— trois mois avant la cessation prévue de la fourniture de services de confiance.

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

([2]) Règlement d'exécution (UE) 2024/3144 de la Commission du 18 décembre 2024 modifiant le règlement d'exécution (UE) 2024/482 en ce qui concerne les normes internationales applicables et rectifiant ledit règlement d'exécution (JO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

6) 7.5 Contrôles cryptographiques

— REQ-EAASP-7.5.2-05: néant

— REQ-EAASP-7.5.2-06: néant

— REQ-EAASP-7.5.3-01A: Des contrôles de sécurité appropriés sont mis en place pour la gestion de toutes les clés cryptographiques, de tous les algorithmes cryptographiques et de tous les dispositifs cryptographiques tout au long de leur cycle de vie, en adoptant, le cas échéant, une approche d'agilité cryptographique.

— REQ-EAASP-7.5.3-01B: Aux fins de la fourniture de ses services de confiance, le prestataire de services d'attestation électronique d'attribut sélectionne et utilise des techniques cryptographiques appropriées conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [2].

— REQ-EAASP-7.5.3-02: Le prestataire de services d'attestation électronique d'attribut veille à ce que le dispositif cryptographique sécurisé qu'il utilise pour la signature ou le cachet numérique de l'attestation électronique d'attribut soit un dispositif de création de signature ou de cachet qualifié et à ce que tous les autres signatures ou cachets numériques utilisés pour fournir le service de confiance pour l'attestation électronique d'attributs correspondant, ou une partie de celui-ci, soient créés au moyen d'un dispositif cryptographique sécurisé qui est un système fiable certifié conformément:

  (a) aux critères communs pour l'évaluation de la sécurité des technologies de l'information, tels qu'ils sont définis dans les critères communs pour l'évaluation de la sécurité des technologies de l'information, version 3.1 (CC3.1) jusqu'au 31.8.2027, ou dans la version CC:2022, parties 1 à 5, publiés par les participants à l'arrangement de reconnaissance mutuelle selon les critères communs dans le domaine de la sécurité informatique, ou dans la norme ISO/IEC 15408 [6], et certifiés au niveau EAL 4 ou supérieur; ou

  (b) au schéma européen commun de certification de cybersécurité fondé sur des critères communs (EUCC) [4][5] et certifié au niveau EAL 4 ou supérieur; ou

  (c) à la norme FIPS-140-2 niveau 3 à utiliser jusqu'au 31.8.2027 pour les systèmes certifiés existants ou à la norme FIPS PUB 140-3 [3] niveau 3 jusqu'au 31.12.2030.

  Cette certification est faite par rapport à une cible de sécurité ou à un profil de protection, ou à une conception de module et une documentation de sécurité, répondant aux exigences du présent document, sur la base d'une analyse des risques et en prenant en compte des mesures de sécurité physiques et d'autres mesures de sécurité non techniques.

  Si le dispositif cryptographique sécurisé bénéficie d'une certification EUCC [4] [5], ce dispositif doit être configuré et utilisé conformément à cette certification.

— REQ-EAASP-7.5.5-01: néant

— REQ-EAASP-7.5.5-02: néant

— REQ-EAASP-7.5.5-04: néant

7) 7.9 Vulnérabilités et gestion des incidents

— REQ-EAASP-7.9-02: Les activités de surveillance tiennent compte de la sensibilité de toute information collectée ou analysée.

8) 7.12 Cessation d'activité et plans de cessation de l'EAASP et de l'EAAS:

— REQ-EAASP-7.12-04: Le plan de cessation d'activité du prestataire de services d'attestation électronique d'attribut satisfait aux exigences énoncées dans les actes d'exécution adoptés en vertu de l'article 24, paragraphe 5, du règlement (UE) nº 910/2014 [i.1].».

ANNEXE II

«*ANNEXE II*

Spécifications techniques visées à l'article 3 et à l'article 4

Les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte délivrent leurs attestations conformément à l'une au moins des normes énumérées à l'annexe II du règlement d'exécution (UE) 2024/2979 de la Commission ([1]) et appliquent les techniques de révocation correspondantes, également énoncées dans l'annexe II du règlement d'exécution (UE) 2024/2979 de la Commission.».

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

ANNEXE III

«ANNEXE IV

Liste des normes et des spécifications techniques mentionnées à l'article 9

Les mécanismes de vérification visés à l'article 9 sont conformes à l'un des éléments suivants, ou aux deux, moyennant les adaptations suivantes:

a) les spécifications techniques énoncées dans la clause 6.1.1 de la norme ETSI TS 119 478 V1.1.1 (2026-01) - Signatures électroniques et infrastructures de confiance (ESI); Spécification des interfaces liées aux sources authentiques;

— REQ-ASIP-6.1.1.2-04-01 [CONDITIONNEL]: Dans le cas où attributeVerificationResult est soit http://uri.etsi.org/19478/VerificationResult/Match soit http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, attributeVerificationResult peut contenir un élément attributeValue.

— REQ-ASIP-6.1.1.2-04-02 [CONDITIONNEL]: Dans le cas où attributeVerificationResult renvoyé est http://uri.etsi.org/19478/VerificationResult/Match et où attributeVerificationResult contient un élément attributeValue, l'élément attributeValue doit contenir la valeur indiquée dans la demande.

— REQ-ASIP-6.1.1.2-04-03 [CONDITIONNEL]: Dans le cas où attributeVerificationResult renvoyé est http://uri.etsi.org/19478/VerificationResult/MatchWithVariation et où attributeVerificationResult contient un élément attributeValue, l'élément attributeValue doit contenir la valeur de l'attribut telle que stockée dans la source authentique.

— REQ-ASIP-6.1.1.2-06-04-01 [CONDITIONNEL]: Dans le cas où fragmentVerificationResult est soit http://uri.etsi.org/19478/VerificationResult/Match soit http://uri.etsi.org/19478/VerificationResult/MatchWithVariation attributeVerificationResult peut contenir un élément fragmentValue.

— REQ-ASIP-6.1.1.2-06-04-02 [CONDITIONNEL]: Dans le cas où fragmentVerificationResult renvoyé est http://uri.etsi.org/19478/VerificationResult/Match et où attributeVerificationResult contient un élément fragmentValue, l'élément fragmentValue doit contenir la valeur indiquée dans la demande.

— REQ-ASIP-6.1.1.2-06-04-03 [CONDITIONNEL]: Dans le cas où fragmentVerificationResult renvoyé est http://uri.etsi.org/19478/VerificationResult/MatchWithVariation et où attributeVerificationResult contient un élément fragmentValue, l'élément fragmentValue doit contenir la valeur du fragment de l'attribut telle que stockée dans la source authentique.

b) les spécifications techniques énoncées dans la clause 6.2.3 de la norme ETSI TS 119 478 V1.1.1 (2026-01) - Signatures électroniques et infrastructures de confiance (ESI); Spécification des interfaces liées aux sources authentiques.

— REQ-ASIP-6.2.3.2.1-08-04: L'élement AttributeVerificationResponse peut contenir exactement un élément enfant au choix entre TextValue, XMLValue ou AttributeProperties.».