Journal officiel
de l'Union européenne

FR
Série L

2025/1945

30.9.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/1945 DE LA COMMISSION

du 29 septembre 2025

portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne la validation des signatures électroniques qualifiées et des cachets électroniques qualifiés et la validation des signatures électroniques avancées reposant sur des certificats qualifiés et des cachets électroniques avancés reposant sur des certificats qualifiés

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 32, paragraphe 3, son article 32 *bis*, paragraphe 3, son article 40 et son article 40 *bis*,

considérant ce qui suit:

(1) Les signatures électroniques qualifiées, les cachets électroniques qualifiés, les signatures électroniques avancées reposant sur des certificats qualifiés de signature électronique et les cachets électroniques avancés reposant sur des certificats qualifiés de cachet électronique, à condition que leur validité puisse être confirmée, garantissent aux parties utilisatrices l'intégrité et l'authenticité des données munies de la signature ou du cachet et renforcent la certitude quant à l'identité du signataire ou du créateur de cachet. Ces signatures électroniques et ces cachets électroniques jouent un rôle crucial dans l'environnement numérique des entreprises en favorisant la transition des processus traditionnels sur support papier vers des processus électroniques équivalents.

(2) La présomption de conformité prévue à l'article 32, paragraphe 1, à l'article 40, à l'article 32 *bis*, paragraphe 3, et à l'article 40 *bis* du règlement (UE) nº 910/2014 devrait s'appliquer lorsque les processus de validation des signatures électroniques qualifiées, des cachets électroniques qualifiés, des signatures électroniques avancées reposant sur des certificats qualifiés de signature électronique et des cachets électroniques avancés reposant sur des certificats qualifiés de cachet électronique sont conformes aux normes techniques énoncées dans le présent règlement. 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 contrôles supplémentaires qui garantissent la capacité de vérifier la validité technique de ces signatures et cachets et, le cas échéant, leur statut qualifié.

(3) La Commission évalue régulièrement de nouvelles technologies, pratiques, normes ou spécifications techniques. Conformément au considérant 75 du règlement (UE) 2024/1183 du Parlement européen et du Conseil ([2]), la Commission devrait réexaminer et, si besoin est, mettre à jour le présent règlement, afin de le maintenir en adéquation avec les évolutions générales, les nouvelles technologies et les normes ou spécifications techniques et de suivre les meilleures pratiques sur le marché intérieur.

(4) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([3]) et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([4]) 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]) 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).

([3]) 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).

([4]) 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).

(5) 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 ([5]) et a rendu son avis le 6 juin 2025.

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

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Normes et spécifications de référence

1. Les normes de référence et les spécifications visées à l'article 32, paragraphe 3, et à l'article 40 du règlement (UE) nº 910/2014 figurent à l'annexe I du présent règlement.

2. Les normes de référence et les spécifications visées à l'article 32 *bis*, paragraphe 3, et à l'article 40 *bis* du règlement (UE) nº 910/2014 figurent à l'annexe II du présent règlement.

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*.

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

Fait à Bruxelles, le 29 septembre 2025.

Par la Commission
La présidente
Ursula VON DER LEYEN

([5]) 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).

ANNEXE I

Liste des normes et spécifications de référence pour la validation des signatures électroniques qualifiées et des cachets électroniques qualifiés

Les normes ETSI TS 119 172-4 V1.1.1 (2021-05) ([1]) («ETSI TS 119 172-4») et ETSI TS 119 102-2 V1.4.1 (2023-06) ([2]) («ETSI TS 119 102-2») s'appliquent moyennant les adaptations suivantes:

1. Pour l'ETSI TS 119 172-4

   1) 2.1 Références normatives:

      — [1] ETSI EN 319 102-1 V1.4.1 (2024-06) Signatures électroniques et infrastructures de confiance (ESI) — Procédures de création et de validation des signatures numériques AdES — Partie 1: création et validation.

      — Toutes les références à «ETSI TS 119 102-1 [1]» s'entendent comme faites à «ETSI EN 319 102-1 [1]».

      — [2] ETSI TS 119 612 V2.3.1 (2024-11) Signatures électroniques et infrastructures (ESI); Listes de confiance.

      — [13] ETSI TS 119 101 V1.1.1 (2016-03) Signatures électroniques et infrastructures (ESI) - Exigences en matière de politique et de sécurité pour les applications de création et de validation de signatures.

   2) 4.2 Contraintes et procédures de validation, exigence REQ-4.2-03, section «contraintes de validation X.509», point c):

      — i) Si un certificat d'entité finale représente une ancre de confiance, il n'y a pas lieu d'utiliser les contraintes RevocationCheckingConstraints.

      — ii) Si un certificat d'entité finale ne représente pas une ancre de confiance, la valeur des contraintes RevocationCheckingConstraints doit être fixée à «eitherCheck» tel que défini dans l'ETSI TS 119 172-1 [3], paragraphe A.4.2.1, tableau A.2, lignes m) 2.1.

      — iii) Si un certificat d'entité finale représente une ancre de confiance, il n'y a pas lieu d'utiliser les contraintes RevocationFreshnessConstraints définies dans l'ETSI TS 119 172-1 [3], paragraphe A.4.2.1, tableau A.2, lignes m) 2.2.

      — iv) Si un certificat d'entité finale ne représente pas une ancre de confiance, les contraintes Revocation-FreshnessConstraints définies dans l'ETSI TS 119 172-1 [3], paragraphe A.4.2.1, tableau A.2, lignes m) 2.2, doivent être utilisées, la valeur maximale étant de 24 heures pour le certificat de signature. Aucune valeur n'est fixée pour les contraintes *RevocationFreshnessConstraints* pour les certificats autres que le certificat de signature, y compris les certificats à l'appui des horodatages.

   3) 4.3 Exigences relatives aux pratiques en matière de validation des signatures et de vérification des règles d'applicabilité

      — REQ-4.3-02: les applications de validation de signature doivent être conformes à l'ETSI TS 119 101 [13].

([1]) ETSI TS 119 172-4 — Signatures électroniques et infrastructures (ESI) — Politiques de signature — Partie 4: (politique de validation des) règles d'applicabilité des signatures pour les signatures électroniques qualifiées et les cachets électroniques qualifiés européens utilisant des listes de confiance, V1.1.1 (2021-05).

([2]) ETSI TS 119 102-2 — Signatures électroniques et infrastructures (ESI) — Procédures de création et de validation des signatures numériques AdES — Partie 2: rapport de validation de signature, V1.4.1 (2023-06).

4) 4.4 Processus de vérification (des règles) de l'applicabilité technique

— REQ-4.4.2-03: si l'une des vérifications prévues par le REQ-4.4.2-01 échoue, alors:

a) le processus s'arrête;

b) la signature doit être techniquement considérée comme indéterminée, c'est-à-dire comme n'étant ni une signature électronique qualifiée de l'UE, ni un cachet électronique qualifié de l'UE; et

c) le résultat ci-dessus et les résultats de tous les processus intermédiaires doivent être pris en compte dans le rapport de vérification relatif aux règles d'applicabilité de la signature.

ANNEXE II

Liste des normes et spécifications de référence pour la validation des signatures électroniques avancées reposant sur des certificats qualifiés et des cachets électroniques avancés reposant sur des certificats qualifiés

Les normes ETSI TS 119 172-4 V1.1.1 (2021-05) ([1]) («ETSI TS 119 172-4») et ETSI TS 119 102-2 V1.4.1 (2023-06) ([2]) («ETSI TS 119 102-2») s'appliquent moyennant les adaptations suivantes:

1. Pour l'ETSI TS 119 172-4

   1) 2.1 Références normatives:

      — [1] ETSI EN 319 102-1 V1.4.1 (2024-06) Signatures électroniques et infrastructures de confiance (ESI) — Procédures de création et de validation des signatures numériques AdES — Partie 1: création et validation.

      — Toutes les références à «ETSI TS 119 102-1 [1]» s'entendent comme faites à «ETSI EN 319 102-1 [1]».

      — [2] ETSI TS 119 612 V2.3.1 (2024-11) Signatures électroniques et infrastructures (ESI) - Listes de confiance.

      — [13] ETSI TS 119 101 V1.1.1 (2016-03) Signatures électroniques et infrastructures (ESI) — Exigences en matière de politique et de sécurité pour les applications de création et de validation de signatures.

   2) 4.2 Contraintes et procédures de validation, exigence REQ-4.2-03, section «contraintes de validation X.509», point c):

      — i) Si un certificat d'entité finale représente une ancre de confiance, il n'y a pas lieu d'utiliser les contraintes *RevocationCheckingConstraints*.

      — ii) Si un certificat d'entité finale ne représente pas une ancre de confiance, la valeur des contraintes *RevocationCheckingConstraints* doit être fixée à «*eitherCheck*» tel que défini dans l'ETSI TS 119 172-1 [3], paragraphe A.4.2.1, tableau A.2, lignes m) 2.1.

      — iii) Si un certificat d'entité finale représente une ancre de confiance, il n'y a pas lieu d'utiliser les contraintes *RevocationFreshnessConstraints* définies dans l'ETSI TS 119 172-1 [3], paragraphe A.4.2.1, tableau A.2, lignes m) 2.2.

      — iv) Si un certificat d'entité finale ne représente pas une ancre de confiance, les contraintes *RevocationFreshnessConstraints* définies dans l'ETSI TS 119 172-1 [3], paragraphe A.4.2.1, tableau A.2, lignes m) 2.2, doivent être utilisées, la valeur maximale étant de 24 heures pour le certificat de signature. Aucune valeur n'est fixée pour les contraintes *RevocationFreshnessConstraints* pour les certificats autres que le certificat de signature, y compris les certificats à l'appui des horodatages.

   3) 4.3 Exigences relatives aux pratiques en matière de validation des signatures et de vérification des règles d'applicabilité

      — REQ-4.3-02: les applications de validation de signature doivent être conformes à l'ETSI TS 119 101 [13].

   4) 4.4 Processus de vérification (des règles) de l'applicabilité technique

      — REQ-4.4.2-03: si l'une des vérifications prévues par le REQ-4.4.2-01 échoue, alors:

         a) le processus s'arrête;

         b) la signature doit être techniquement déterminée comme étant indéterminée, c'est-à-dire comme n'étant ni une signature électronique avancée fondée sur un certificat qualifié de l'UE, ni un cachet électronique avancé fondé sur un certificat qualifié de l'UE; et

([1]) ETSI TS 119 172-4 — Signatures électroniques et infrastructures (ESI) — Politiques de signature — Partie 4: (politique de validation des) règles d'applicabilité des signatures pour les signatures électroniques qualifiées et les cachets électroniques qualifiés européens utilisant des listes de confiance, V1.1.1 (2021-05).

([2]) ETSI TS 119 102-2 — Signatures électroniques et infrastructures (ESI) — Procédures de création et de validation des signatures numériques AdES — Partie 2: rapport de validation de signature, V1.4.1 (2023-06).

c) le résultat ci-dessus et les résultats des processus de tous les processus intermédiaires doivent être pris en compte dans le rapport de vérification relatif aux règles d'applicabilité de la signature.

— REQ-4.4.2-04: vide.

— REQ-4.4.2-05: vide.

— REQ-4.4.2-06: à ce stade du processus de vérification (des règles) de l'applicabilité technique (TARC), si les conditions suivantes sont remplies:

a) le certificat de signature est déterminé, au «best signature time», comme étant un certificat qualifié de signature électronique (ou de cachet électronique, selon le cas) de l'UE, comme spécifié dans le REQ-4.4.2-02, point a); et

b) le résultat du processus exécuté conformément au paragraphe 4.2 du présent document est TOTAL-PASSED,

alors la signature numérique doit être déterminée comme étant techniquement appropriée pour mettre en œuvre une signature électronique avancée de l'UE fondée sur un certificat qualifié (ou un cachet électronique avancé de l'UE fondé sur un certificat qualifié, selon le cas), sinon la signature n'est pas déterminée techniquement ni comme une signature électronique avancée de l'UE fondée sur un certificat qualifié, ni comme un cachet électronique avancé de l'UE fondé sur un certificat qualifié.