Journal officiel
de l'Union européenne

FR
Série L

2025/1946

30.9.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/1946 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 les services qualifiés de préservation des signatures électroniques qualifiées et des cachets électroniques 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 34, paragraphe 2, et son article 40,

considérant ce qui suit:

(1) Les services qualifiés de préservation des signatures électroniques qualifiées et des cachets électroniques qualifiés garantissent, sur le long terme, l'intégrité, l'authenticité, la preuve de l'existence et l'accessibilité des preuves de préservation de ces signatures électroniques et cachets électroniques. Cela permet de démontrer leur validité juridique sur des périodes prolongées et garantit la possibilité de les valider, quelles que soient les évolutions technologiques futures. Ces services sont fournis de manière indépendante ou dans le cadre d'un autre service de confiance qualifié, tel que des services d'archivage électronique qualifiés.

(2) La présomption de conformité prévue à l'article 34, paragraphe 1 *bis*, et à l'article 40 du règlement (UE) nº 910/2014 ne devrait s'appliquer que lorsque les services qualifiés de préservation des signatures électroniques qualifiées et des cachets électroniques qualifiés sont conformes aux normes 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 sécurité et la fiabilité du service de confiance qualifié, ainsi que la capacité de vérifier le statut qualifié et la validité technique des signatures et des cachets au fil du temps.

(3) Si un prestataire de services de confiance respecte les exigences énoncées à l'annexe du présent règlement, les organes de contrôle devraient présumer que les exigences pertinentes du règlement (UE) nº 910/2014 sont respectées et tenir dûment compte de cette présomption pour l'octroi ou la confirmation du statut qualifié du service de confiance. Toutefois, un prestataire de services de confiance qualifiés peut toujours s'appuyer sur d'autres pratiques pour démontrer le respect des exigences du règlement (UE) nº 910/2014.

(4) 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.

([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).

(5) 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.

(6) 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.

(7) 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

Normes et spécifications de référence

Les normes de référence et les spécifications visées à l'article 34, paragraphe 2, et à l'article 40 du règlement (UE) nº 910/2014 figurent à l'annexe 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

([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]) 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

Liste des normes de référence et des spécifications mentionnées à l'article 2

Les normes ETSI TS 119 511 V1.1.1 (2019-06) («ETSI TS 119 511») et ETSI TS 119 172-4 V1.1.1 (2021-05) («ETSI TS 119 172-4») s'appliquent moyennant les adaptations suivantes:

1. Pour ETSI TS 119 511

1) 2.1 Références normatives:

— [1] ETSI TS 319 401 V3.1.1 (2024-06) «Signatures électroniques et infrastructures (ESI) — Exigences de politique générale applicables des prestataires de services de confiance».

— [2] ETSI TS 119 612 (V2.3.1) «Electronic Signatures and Infrastructures (ESI); Trusted Lists».

— [5] FIPS PUB 140-3 (2019) «Security Requirements for Cryptographic Modules».

— [6] Règlement d'exécution (UE) 2024/482 de la Commission ([1]) 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).

— [7] Règlement d'exécution (UE) 2024/3144 de la Commission ([2]) modifiant le règlement d'exécution (UE) 2024/482 en ce qui concerne les normes internationales applicables et rectifiant ledit règlement d'exécution.

— [8] 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]).

— [9] ETSI TS 119 172-4 V1.1.1 (2021-05) «Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists».

— [10] 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

— 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) 6.4 Profils de préservation

— OVR-6.4-08A [WTS] [WOS] La durée attendue des preuves doit être conforme aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [8].

— NOTE 3 vide.

4) 6.5 Politique de préservation des éléments de preuve

— OVR-6.5-04A Les algorithmes cryptographiques utilisés doivent être conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [8].

— NOTE 1 vide.

([1]) JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([2]) JO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

5) 7.2 Ressources humaines

— OVR-7.2-02 Le personnel employé par le PSP (fournisseur du service de préservation) dans des rôles de confiance et, le cas échéant, les sous-traitants du PSP intervenant dans des rôles de confiance, doivent être en mesure de satisfaire à l'exigence concernant les «connaissances spécialisées, l'expérience et les qualifications» grâce à une formation formelle et à des certificats, ou de manière empirique, ou par une combinaison des deux.

— OVR-7.2-03 La conformité au point OVR-7.2-02 doit impliquer des mises à jour régulières (au moins tous les 12 mois) sur les nouvelles menaces et les pratiques actuelles en matière de sécurité.

6) 7.5 Contrôles cryptographiques

— OVR-7.5-05 [CONDITIONNEL] Lorsque le PSP signe (une partie d') une preuve de préservation, la clé de signature privée du PSP doit être stockée et utilisée dans 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 la norme ISO/IEC 15408 [10] ou dans les critères communs pour l'évaluation de la sécurité des technologies de l'information, 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 et certifiés au niveau EAL 4 ou supérieur; ou

b) à l'EUCC [6] [7] et certifié au niveau EAL 4 ou supérieur; ou

c) jusqu'au 31.12.2030, à la norme FIPS PUB 140-3 [5] niveau 3.

Cette certification doit être 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 [6] [7], ce dispositif doit être configuré et utilisé conformément à cette certification.

— OVR-7.5-06 [CONDITIONNEL] vide.

— OVR-7.5-07 [CONDITIONNEL] Lorsque le PSP signe (une partie d') une preuve de préservation, les éventuelles copies de sauvegarde des clés de signature privée du PSP doivent être protégées afin que leur intégrité et leur confidentialité soient garanties par le dispositif cryptographique sécurisé, avant qu'elles soient stockées à l'extérieur de ce dispositif.

— OVR-7.5-08 Toute exportation ou importation de clé de signature privée d'un PSP à partir ou à destination d'un autre dispositif cryptographique doit être mise en œuvre de manière sécurisée et conformément à la certification de ces dispositifs.

7) 7.8 Sécurité du réseau

— OVR-7.8-03 L'analyse de vulnérabilité requise en vertu du REQ-7.8-13 de la norme ETSI EN 319 401 [1] doit être effectuée au moins une fois par trimestre.

— OVR-7.8-04 Le test d'intrusion requis en vertu du REQ-7.8-17X de la norme ETSI EN 319 401 [1] doit être effectué au moins une fois par an.

— OVR-7.8-05 Les pare-feu doivent être configurés de manière à empêcher tous les protocoles et accès non nécessaires au fonctionnement du PSP.

8) 7.14 Surveillance cryptographique

— OVR-7.14-03A L'évaluation des algorithmes cryptographiques dans OVR-7.14.01 et OVR-7.14.02 est conforme aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [8].

— NOTE vide.

9) 7.12 Cessation d'activité et plans de cessation du TSP

— OVR-7.12-01A Le plan de cessation d'activité du TSP doit satisfaire aux exigences énoncées dans les actes d'exécution adoptés en vertu de l'article 24, paragraphe 5, du règlement (UE) nº 910/2014 [i.2].

10) 7.17 Chaîne d'approvisionnement

— OVR-7.17-01 Les exigences spécifiées dans l'ETSI EN 319 401 [1], paragraphe 7.14, doivent s'appliquer.

11) Annexe A (normative): Service qualifié de préservation pour QES au sens de l'article 34 du règlement (UE) nº 910/2014

— OVR-A-02 [PDS] [PDS + PGD]

a) le service de préservation doit conserver toutes les informations nécessaires pour vérifier le statut qualifié de la signature ou du cachet électronique, qui ne seraient pas accessibles au public avant la fin de la période de préservation;

b) le service de préservation doit veiller à ce que, à tout moment au cours de la période de préservation, les informations préservées soient telles que, lorsqu'elles sont fournies pour alimenter le processus spécifié dans l'ETSI TS 119 172-4 [9], paragraphe 4.4, le résultat de ce processus détermine clairement si la signature ou le cachet numérique étaient, au moment de leur préservation, techniquement appropriés pour la mise en œuvre d'une signature électronique qualifiée de l'UE ou d'un cachet électronique qualifié de l'UE.

— OVR-A-03 [PDS] [PDS + PGD] Il convient que les horodatages utilisés dans les preuves de préservation soient des horodatages qualifiés conformément au règlement (UE) nº 910/2014 [i.2].

2. Pour 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 (ESI) — Modes opératoires pour la création et la 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) «Electronic Signatures and Infrastructures (ESI); Trusted Lists».

— [13] ETSI TS 119 101 V1.1.1 (2016-03) «Electronic Signatures and Infrastructures (ESI) — Policy and security requirements for applications for signature creation and signature validation».

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 0 pour le certificat de signature, en veillant à ce que les informations de révocation ne soient acceptées que si elles ont été délivrées après le *best signature time*. 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 REQ-4.4.2-01 échoue, alors:

— le processus s'arrête;

— 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;

— 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.