Journal officiel
de l'Union européenne

FR
Série L

2025/1942

30.9.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/1942 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 de validation qualifiés des signatures électroniques qualifiées et les services de validation qualifiés 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 33, paragraphe 2, et son article 40,

considérant ce qui suit:

(1) Les services de validation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés garantissent l'intégrité, l'authenticité et la correction du processus et des résultats de la validation, respectivement, des signatures électroniques qualifiées et des cachets électroniques qualifiés. Ces services de confiance qualifiés 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 33, paragraphe 2, et à l'article 40 du règlement (UE) nº 910/2014 ne devrait s'appliquer que lorsque les services de validation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés 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 sécurité et la fiabilité des service de confiance qualifiés, ainsi que la capacité de vérifier le statut qualifié et la validité technique des signatures électroniques qualifiées et des cachets électroniques qualifiés.

(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 aux 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 institué 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 33, 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 et spécifications de référence pour les services de validation qualifiés des signatures électroniques qualifiées et les services de validation qualifiés des cachets électroniques qualifiés

Les normes ETSI TS 119 441 V1.2.1 (2023-10) ([1]) («ETSI TS 119 441») et ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) («ETSI TS 119 172-4») s'appliquent moyennant les adaptations suivantes:

1. Pour l'ETSI TS 119 441

   1) 2.1 Références normatives

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

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

   — [4] ISO/IEC 15408-1:2022 – Sécurité de l'information, cybersécurité et protection de la vie privée – Critères d'évaluation pour la sécurité des technologies de l'information.

   — [5] vide

   — [6] FIPS PUB 140-3 (2019) Exigences de sécurité pour les modules cryptographiques.

   — [7] Règlement d'exécution (UE) 2024/482 de la Commission ([3]) 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).

   — [8] ETSI TS 119 172-4 V1.1.1 (2021-05) 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.

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

   — [10] Groupe européen de certification de cybersécurité, sous-groupe sur la cryptographie: mécanismes cryptographiques agréés («Agreed Cryptographic Mechanisms»), publié par l'Agence de l'Union européenne pour la cybersécurité (ENISA) ([4]).

   — [11] Règlement d'exécution (UE) 2024/3144 de la Commission ([5]) modifiant le règlement d'exécution (UE) 2024/4822 en ce qui concerne les normes internationales applicables et rectifiant ledit règlement d'exécution.

   — [12] ETSI EN 319 411-1 Signatures électroniques et infrastructures (ESI) – Exigences de politique et de sécurité applicables aux prestataires de services de confiance délivrant des certificats – Partie 1: exigences générales

([1]) ETSI TS 119 441 – Signatures électroniques et infrastructures (ESI) – Exigences en matière de politique applicables au prestataire de services de confiance fournissant des services de validation de signature, V1.2.1 (2023-10).

([2]) 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).

([3]) JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.

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

([5]) JO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 2.2 Références normatives

— [I.11] vide.

3) 3.3 Abréviations

— EUCC Schéma européen de certification de cybersécurité fondé sur des critères communs

4) 4.3.3 Processus

— REMARQUE 10: voir l'ETSI EN 319 102-1 [3] pour des orientations et l'ETSI TS 119 172-4 [8] pour des orientations supplémentaires aux fins de la signature qualifiée de l'UE ou du cachet qualifié de l'UE.

5) 6.1 Déclaration des pratiques du service de validation de signature

— OVR-6.1-02: la déclaration des pratiques du SVS doit être structurée comme prévu à l'annexe A.

— OVR-6.1-03: la déclaration des pratiques du SVS doit énumérer les politiques de SVS prises en charge ou y faire référence (par exemple au moyen d'OID) et les décrire brièvement.

6) 6.3 Politique en matière de sécurité de l'information

— OVR-6.3-02: la politique de sécurité doit documenter les contrôles de sécurité et de respect de la vie privée mis en œuvre pour protéger les données à caractère personnel.

7) 7.2 Ressources humaines

— OVR-7.2-02: le personnel des SVSP intervenant dans des rôles de confiance et, le cas échéant, leurs sous-traitants intervenant dans des rôles de confiance doivent pouvoir satisfaire à l'exigence en matière de «connaissances spécialisées, expérience et 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 implique des mises à jour régulières (au moins tous les 12 mois) portant sur les nouvelles menaces et les pratiques actuelles en matière de sécurité.

8) 7.5 Contrôles cryptographiques

— OVR-7.5-02 [CONDITIONNEL]: lorsque les rapports de validation sont signés, le certificat de signature public du SVSP correspondant à la clé de signature privée du SVSP doit être délivré par une autorité de certification digne de confiance, conformément à la politique de certification normalisée «NCP+» définie dans l'ETSI EN 319 411-1 [12]. Il devrait être délivré conformément à une politique de certification appropriée spécifiée dans l'ETSI EN 319 411-2 [i.17].

— OVR-7.5-03 [CONDITIONNEL]: lorsque les rapports de validation sont signés, la clé de signature privée du SVSP doit être conservée 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 [4] 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 [7] [11], et certifié au niveau EAL 4 ou supérieur; ou

c) jusqu'au 31.12.2030, FIPS PUB 140-3 [6] niveau 3.

Cette certification doit être faite par rapport à une cible de sécurité ou 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 autres mesures de sécurité non techniques.

Si le dispositif cryptographique sécurisé bénéficie d'une certification EUCC [7] [11], ce dispositif doit être configuré et utilisé conformément à cette certification.

— OVR-7.5-04: vide.

— OVR-7.5-06: toute exportation ou importation de clé de signature privée d'un SVSP 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.

9) 7.7 Sécurité de fonctionnement

— OVR-7.7-02: afin de garantir que les systèmes sur lesquels l'application est développée appliquent des mesures de sécurité appropriées et s'adaptent aux environnements applicatifs spécifiques, l'application de vérification de signature doit utiliser un environnement applicatif tenu à jour avec des correctifs de sécurité actualisés.

— OVR-7.7-03: les exigences suivantes spécifiées dans l'ETSI TS 119 101 [1], paragraphe 5.2, s'appliquent à l'application de validation de signature: GSM 1.3.

10) 7.8 Sécurité du réseau

— OVR-7.8-02: si l'accès à distance aux systèmes de stockage ou de traitement de données confidentielles est autorisé, une politique formelle doit être adoptée et décrite dans le cadre des éléments requis par l'OVR-6.3-02.

— OVR-7.8-04: l'analyse de vulnérabilité requise en vertu du REQ-7.8-13 de l'ETSI EN 319 401 [1] doit être effectuée au moins une fois par trimestre.

— OVR-7.8-05: le test d'intrusion requis en vertu du REQ-7.8-17X de l'ETSI EN 319 401 [1] doit être effectué au moins une fois par an.

— OVR-7.8-06: les pare-feu doivent être configurés de manière à empêcher tous les protocoles et accès non nécessaires au fonctionnement du SVSP.

11) 7.12 Plans d'arrêt de fourniture et d'arrêt d'activité du service de validation de signature

— OVR-7.12-02: le plan d'arrêt d'activité du prestataire de services de confiance 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.1].

12) 7.14 Chaîne d'approvisionnement

— OVR-7.14-01: les exigences spécifiées dans l'ETSI EN 319 401 [2], paragraphe 7.14, s'appliquent.

13) 8.1 Processus de validation des signatures

— VPR-8.1-07: l'application de validation (SVA) doit être conforme aux exigences de l'ETSI TS 119 101 [1], paragraphe 7.4, SIA 1 à SIA 4.

— VPR-8.1-11 [CONDITIONNEL]: si le SVS a pour objet de valider des signatures électroniques qualifiées ou des cachets électroniques qualifiés conformément à l'article 32, paragraphe 1, (ou à l'article 40, selon le cas) du règlement (UE) nº 910/2014 [i.1], le processus de validation doit respecter les exigences de l'ETSI TS 119 172-4 [8].

14) 8.2 Protocole de validation des signatures

— SVP-8.2-03: la réponse de validation de signature doit comporter l'identifiant OID de la politique du SVS.

15) 8.4 Rapport de validation des signatures

— SVR-8.4-02: le rapport de validation doit être conforme à l'ETSI TS 119 102-2 [9].

— SVR-8.4-07 [CONDITIONNEL]: si une politique de validation de signature n'est pas entièrement traitée par le SVS, le rapport doit, outre les contraintes validées, rendre compte des contraintes qui ont été ignorées ou écartées.

— SVR-8.4-15: le rapport de validation doit indiquer clairement l'origine de chaque preuve d'existence (PoE) (au départ de la signature proprement dite, du client, du serveur).

— SVR-8.4-16: le rapport de validation doit être revêtu d'une signature de rapport de validation, qui doit être la signature numérique du SVSP.

— SVR-8.4-17 [CONDITIONNEL]: lorsque les rapports de validation sont signés, le format et la cible de la signature doivent être conformes à l'ETSI TS 119 102-2 [9].

16) 9 Cadre pour la définition des politiques en matière de services de validation fondées sur une politique de services de confiance définie dans le présent document:

— OVR-9-05 [CONDITIONNEL]: lorsqu'une politique de SVS est élaborée sur la base d'une politique de services de confiance définie dans le présent document, une évaluation des risques doit être effectuée afin d'évaluer les exigences opérationnelles et de déterminer les exigences de sécurité à inclure dans la politique applicable à la communauté et à l'applicabilité déclarées.

— OVR-9-06 [CONDITIONNEL]: lorsqu'une politique de SVS est élaborée sur la base d'une politique de services de confiance définie dans le présent document, la politique doit être approuvée et modifiée selon un processus de réexamen défini, comprenant les responsabilités en matière de maintien de la politique.

— OVR-9-07 [CONDITIONNEL]: lorsqu'une politique de SVS est élaborée sur la base d'une politique de services de confiance définie dans le présent document, il doit exister un processus de réexamen défini pour garantir que la politique est prise en charge par les déclarations de pratiques.

— OVR-9-08 [CONDITIONNEL]: lorsqu'une politique de SVS est élaborée sur la base d'une politique de services de confiance définie dans le présent document, le prestataire de services de confiance doit mettre les politiques qu'il prend en charge à la disposition de sa communauté d'utilisateurs.

— OVR-9-09 [CONDITIONNEL]: lorsqu'une politique de SVS est élaborée sur la base d'une politique de services de confiance définie dans le présent document, les révisions apportées aux politiques prises en charge par le prestataire de services de confiance doivent être mises à la disposition des abonnés.

17) Annexe B (normative) – Service de validation qualifié des signatures électroniques qualifiées au sens de l'article 33 du règlement (UE) n° 910/2014:

— VPR-B-02 [CONDITIONNEL]: si le SVSP est un QSVSP, la mise en œuvre doit être conforme à l'ETSI TS 119 172-4 [8].

— REMARQUE 2: vide.

— OVR-B-04 [CONDITIONNEL]: si le SVSP est un QSVSP, les tests prévus dans l'OVR-B-03 doivent vérifier différents cas d'utilisation, positifs et négatifs.

— VPR-B-11 [CONDITIONNEL]: si le SVSP est un QSVSP, le SVSP doit contrôler le calcul de hachage (soit effectuer le calcul du côté serveur, soit contrôler le client s'il y est autorisé du côté client).

— REMARQUE 5: vide.

— REMARQUE 6: vide.

— VPR-B-15 [CONDITIONNEL]: si le SVSP est un QSVSP, afin de satisfaire aux exigences des VPR-B-13 à VPR-B-14, le rapport de validation doit être conforme à l'ETSI TS 119 102-2 [9].

— VPR-B-16 [CONDITIONNEL]: si le SVSP est un QSVSP, la mise en œuvre doit être conforme aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [10] pour l'utilisation de techniques cryptographiques appropriées lors de la fourniture de services de validation qualifiés des signatures électroniques qualifiées.

18) Annexe C (informative) – Mise en correspondance des exigences avec le règlement (UE) nº 910/2014, section «Fourniture d'une validation en conformité avec l'article 32, paragraphe 1», deuxième alinéa:

— Afin de garantir que toutes les conditions requises par l'article 32, paragraphe 1, et l'article 40 du règlement (UE) nº 910/2014 [i.1] sont vérifiées, un algorithme de validation correct est nécessaire. Il fournit le même résultat déterministe pour une signature ou un cachet soumis à validation. La politique de validation de signature est essentielle à cette fin. L'ETSI TS 119 172-4 [8], sur la base de l'algorithme de validation spécifié dans l'ETSI EN 319 102-1 [3], a été publiée dans cette perspective.

2. 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* dans le cas de certificats autres que le certificat de signature, y compris les certificats à l'appui des horodatages.

3) 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;

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