Journal officiel
de l'Union européenne

FR
Série L

2025/1567

30.7.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/1567 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 la gestion des dispositifs de création de signature électronique qualifiés à distance et des dispositifs de création de cachets électroniques qualifiés à distance en tant que services de confiance

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 29 *bis*, paragraphe 2, et son article 39 *bis*,

considérant ce qui suit:

(1) Les services de confiance qualifiés pour la gestion des dispositifs de création de signature électronique qualifiés à distance et pour la gestion des dispositifs de création de cachet électronique qualifiés à distance jouent un rôle crucial dans l'environnement numérique des entreprises en favorisant la transition des processus traditionnels sur support papier vers des équivalents électroniques. Ces services de confiance qualifiés contribuent à une gestion sûre et fiable de ces dispositifs à distance pour le compte des signataires et des créateurs de cachets, de manière à garantir que les conditions relatives aux signatures électroniques qualifiées et aux cachets électroniques qualifiés sont remplies.

(2) Afin de renforcer la sécurité juridique et la fiabilité des services de confiance qualifiés pour la gestion des dispositifs de création de signature électronique qualifiés à distance et des services de confiance qualifiés pour la gestion des dispositifs de création de cachet électronique qualifiés à distance, les prestataires de services de confiance qualifiés fournissant ces services qualifiés devraient se conformer aux normes énoncées dans le présent règlement.

(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 contrôles qui permettent de garantir la sécurité et la fiabilité des services de confiance qualifiés, ainsi qu'à faire en sorte que les signataires exercent un contrôle exclusif, avec un niveau élevé de confiance, sur l'utilisation de leurs données de création de signature électronique, et à ce que les créateurs du cachet aient le contrôle de l'utilisation de leurs données de création de cachet électronique, respectivement.

(4) Afin de garantir un délai suffisant pour l'audit des prestataires de services de confiance en ce qui concerne le respect des nouvelles exigences, le présent règlement devrait s'appliquer à partir de 24 mois à compter de son entrée en vigueur.

(5) 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).

(6) 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.

(7) 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.

(8) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) n° 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Normes et spécifications de référence

Les normes et spécifications de référence pour la gestion des dispositifs de création de signature électronique qualifiés à distance et des dispositifs de création de cachet électronique qualifiés à distance en tant que services de confiance qualifiés visés à l'article 29 *bis*, paragraphe 2, et à l'article 39 *bis* du règlement (UE) n° 910/2014 figurent à l'annexe du présent règlement.

Article 2

Entrée en vigueur et applicabilité

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Il est applicable à partir du 19 août 2027.

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

Fait à Bruxelles, le 29 juillet 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) n° 45/2001 et la décision n° 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 la gestion des dispositifs de création de signature électronique qualifiés à distance et des dispositifs de création de cachet électronique qualifiés à distance

La norme ETSI TS 119 431-1 V1.3.1 (2024-12) (ci-après «ETSI TS 119 431-1») s'applique aux fins de l'évaluation de la conformité avec la politique du service d'application de serveur de signature électronique *EU Server Signing Application Service v2* (SSASP), conformément à l'annexe A de ladite norme, moyennant les adaptations suivantes:

1) 2.1 Références normatives

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

— [7] 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) ([1]).

2) 6.1 Responsabilités en matière de publication et de répertoire

— OVR-6.1-04: les informations mentionnées au point OVR-6.1-01 sont mises à la disposition du public au niveau international.

3) 6.4.4 Contrôles relatifs au personnel

— OVR-6.4.4-02: les SSASP emploient du personnel intervenant dans des rôles de confiance et, le cas échéant, des sous-traitants intervenant dans des rôles de confiance, qui ont acquis les connaissances spécialisées, l'expérience et les qualifications nécessaires grâce à une formation formelle et à des certificats, ou de manière empirique, ou par une combinaison des deux.

— OVR-6.4.4-03: la conformité au point OVR-6.4.4-02 implique des mises à jour régulières (au moins tous les 12 mois) sur les nouvelles menaces et les pratiques actuelles en matière de sécurité.

4) 6.4.9 Arrêt de service de la SSASP

— OVR-6.4.9-02: le plan d'arrêt de la SSASP satisfait aux exigences énoncées dans les actes d'exécution adoptés en vertu de l'article 24, paragraphe 5, du règlement (UE) n° 910/2014 [i.1].

5) 6.5.5 Contrôles de sécurité du réseau

— OVR-6.5.5-02: 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-6.5.5-03: les pare-feu doivent être configurés de manière à empêcher tous les protocoles et accès non nécessaires au fonctionnement du prestataire de service de confiance.

6) 6.8.5 Contrôles cryptographiques

— OVR-6.8.5-01: des contrôles de sécurité appropriés sont mis en place pour la gestion de toutes les techniques cryptographiques de la SSASP tout au long de leur cycle de vie.

— OVR-6.8.5-02: en ce qui concerne l'OVR-6.8.5-01, la SSASP 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 [7].

7) Annexe A, section A.3 Exigences générales

— OVR-A.3-02 [EUSPv2]: la déclaration en matière de pratique du prestataire de services de confiance inclut la référence à la certification du dispositif de création de signature/cachet électronique qualifié employé conformément aux exigences de l'annexe II du règlement (UE) n° 910/2014 [i.1].

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