Journal officiel
de l'Union européenne

FR
Série L

2025/1944

30.9.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/1944 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 normes de référence applicables aux processus d'envoi et de réception de données dans le cadre de services d'envoi recommandé électronique qualifiés et en ce qui concerne l'interopérabilité de ces services

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 44, paragraphe 2, et son article 44, paragraphe 2 *ter*,

considérant ce qui suit:

(1) Les services d'envoi recommandé électronique qualifiés constituent un canal sécurisé pour la transmission de documents, y compris pour la preuve de l'envoi et de la réception des données. Ils visent à certifier l'identification du destinataire et à garantir avec un degré de confiance élevé l'identification de l'expéditeur.

(2) La présomption de conformité prévue à l'article 44, paragraphe 1 *bis*, du règlement (UE) nº 910/2014 ne devrait s'appliquer que lorsque les services de confiance qualifiés de fourniture de services d'envoi recommandé électronique 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.

(3) Si un prestataire de services de confiance respecte les exigences énoncées à l'annexe I 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) Conformément à l'article 44, paragraphe 2 *bis*, du règlement (UE) nº 910/2014, lorsque des prestataires de services de confiance qualifiés conviennent de rendre leurs services interopérables, il importe qu'ils respectent des normes et spécifications appropriées énoncées à l'annexe II du présent règlement d'exécution afin de pouvoir facilement transférer les données faisant l'objet d'un envoi recommandé électronique entre deux ou plusieurs prestataires de services de confiance qualifiés et de promouvoir des pratiques loyales dans le marché intérieur.

(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 institué par l'article 48 du règlement (UE) n° 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Normes de référence et spécifications pour les services d'envoi recommandé électronique qualifiés

Les normes de référence et les spécifications mentionnées à l'article 44, paragraphe 2, du règlement (UE) n° 910/2014 figurent à l'annexe I du présent règlement.

Article 2

Normes de référence et spécifications pour l'interopérabilité entre les services d'envoi recommandé électronique qualifiés

Les normes de référence et les spécifications visées à l'article 44, paragraphe 2 *ter*, du règlement (UE) n° 910/2014 figurent à l'annexe II du présent règlement.

Article 3

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) 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 I

Liste des normes de référence et des spécifications mentionnées à l'article 1er

La norme ETSI EN 319 521 V1.1.1 (2019-02) («ETSI EN 319 521») s'applique moyennant les adaptations suivantes:

1. Pour l'ETSI EN 319 521

   1) 2.1 Références normatives:

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

   — [2] ETSI EN 319 411-1 V1.5.1 (2025-04) 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.

   — [3] ETSI EN 319 522-1 V1.2.1 (2024-01) Signatures électroniques et infrastructures (ESI) — Services d'envoi recommandé électronique — Partie 1: cadre et architecture.

   — [4] ETSI EN 319 522-2 V1.2.1 (2024-01) Signatures électroniques et infrastructures (ESI) — Services d'envoi recommandé électronique — Partie 2: contenu sémantique.

   — [5] 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) ([1]).

   — [6] 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.

   — [7] Règlement d'exécution (UE) 2024/482 de la Commission ([2]) 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] Règlement d'exécution (UE) 2024/3144 de la Commission ([3]) modifiant le règlement d'exécution (UE) 2024/482 en ce qui concerne les normes internationales applicables et rectifiant ledit règlement d'exécution.

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

   2) 3.1 Terminologie

   — Cachet électronique avancé: tel que défini dans le règlement (UE) nº 910/2014 [i.1].

   — Signature électronique avancée: telle que définie dans le règlement (UE) nº 910/2014 [i.1].

   — Cachet électronique qualifié: tel que défini dans le règlement (UE) nº 910/2014 [i.1].

   — Signature électronique qualifiée: telle que définie dans le règlement (UE) nº 910/2014 [i.1].

   — 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.

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

3) 5.1.1 Dispositions communes

— REQ-ERDS-5.1.1-01: l'ERDS doit veiller à ce que la disponibilité, l'intégrité et la confidentialité du contenu des utilisateurs soient suffisamment garanties lors de son traitement par l'ERDS, en assurant l'intégrité et la confidentialité par une sélection de techniques cryptographiques appropriées conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [5].

4) 5.2.1.1 Généralités

— REQ-QERDS-5.2.1.1-01: le QERDSP doit vérifier avec un niveau de confiance très élevé l'identité du destinataire, soit directement, soit en ayant recours à un tiers, et en utilisant l'un des moyens suivants ou une combinaison des moyens suivants, selon le cas:

a) au moyen de la présence en personne de la personne physique ou d'un représentant autorisé de la personne morale, en recourant aux preuves et procédures appropriées, conformément au droit national;

b) à distance, à l'aide d'un moyen d'identification électronique satisfaisant aux exigences énoncées à l'article 8 du règlement (UE) n° 910/2014 [i.1] en ce qui concerne le niveau de garantie «élevé», ou au moyen du portefeuille européen d'identité numérique;

c) au moyen d'un certificat de signature électronique qualifiée ou de cachet électronique qualifié;

d) à l'aide d'autres méthodes d'identification qui garantissent que la personne physique ou le représentant autorisé de la personne morale peuvent être identifiés avec un degré de confiance très élevé. La garantie que cette identification est effectuée avec un degré de confiance très élevé doit être confirmée par un organisme d'évaluation de la conformité.

— REQ-QERDS-5.2.1.1-01A: le QERDSP doit vérifier l'identité de l'expéditeur par des moyens appropriés, soit directement, soit en ayant recours à un tiers, sur la base de l'une des méthodes suivantes ou d'une combinaison des méthodes suivantes:

a) au moyen de la présence en personne de la personne physique ou d'un représentant autorisé de la personne morale, en recourant aux preuves et procédures appropriées, conformément au droit national;

b) à distance, à l'aide du portefeuille européen d'identité numérique ou d'un moyen d'identification électronique notifié satisfaisant aux exigences énoncées à l'article 8 du règlement (UE) n° 910/2014 [i.1] en ce qui concerne le niveau de garantie «substantiel», à condition qu'il ait été délivré sur la base de la présence physique préalable de la personne physique ou d'un représentant autorisé de la personne morale;

c) au moyen d'un certificat de signature électronique avancée ou de cachet électronique avancé, à condition que le certificat ait été délivré à la personne physique ou à un représentant autorisé de la personne morale selon la politique de certification normalisée telle que définie dans l'ETSI EN 319 411-1 [2]; ou

d) à l'aide d'autres méthodes d'identification qui garantissent que la personne physique ou le représentant autorisé de la personne morale peuvent être identifiés avec un degré de confiance très élevé. La garantie que cette identification est effectuée avec un degré de confiance élevé doit être confirmée par un organisme d'évaluation de la conformité.

— REMARQUE: le tiers qui vérifie l'identité de l'expéditeur et du destinataire peut être un autre QERDSP si l'expéditeur et le destinataire sont abonnés à des QERDSP différents.

5) 5.2.1.2 Identification du destinataire et transmission du contenu des utilisateurs

— REQ-QERDS-5.2.1.2-03: si l'identification du destinataire repose sur un processus interne du QERDS, le QERDSP exécute l'ensemble du processus dans un environnement sécurisé et contrôlé.

6) 5.2.2 Dispositions relatives à l'authentification des QERDS de l'UE

— REQ-QERDS-5.2.2-03 [CONDITIONNEL]: si le QERDSP lie des moyens d'authentification à une identité d'expéditeur vérifiée conformément au paragraphe 5.2.1, il doit s'agir de l'un des éléments suivants:

a) des mécanismes d'authentification à deux facteurs;

b) le portefeuille européen d'identité numérique ou un moyen d'identification électronique notifié qui satisfait aux exigences énoncées à l'article 8 du règlement (UE) nº 910/2014 [i.1] en ce qui concerne le niveau de garantie «élevé» ou «substantiel»;

c) une authentification TLS mutuelle, qui comprend le certificat délivré à l'expéditeur selon la politique de certification normalisée telle que définie dans l'ETSI EN 319 411-1 [2];

d) une signature numérique étayée par un certificat délivré selon la politique de certification normalisée telle que définie dans l'ETSI EN 319 411-1 [2];

e) d'autres moyens garantissant l'authentification de l'expéditeur identifié. La conformité de l'établissement du lien est confirmée par un organisme d'évaluation de la conformité. Exemple: cela peut inclure l'utilisation de l'un des moyens visés aux points a), b) et d) ci-dessus pour enregistrer un certificat de client TLS (Transport Layer Security) afin de procéder à des envois automatisés par TLS mutuelle ou pour enregistrer un certificat de cachet numérique afin d'apposer un cachet sur des affirmations d'authentification auprès de l'ERDS. D'autres mécanismes dans lesquels les expéditeurs identifiés ont recours à des services tiers délégués peuvent également être appliqués.

— REQ-QERDS-5.2.2-03A [CONDITIONNEL]: si le QERDSP lie des moyens d'authentification à l'identité d'un destinataire vérifiée conformément au paragraphe 5.2.1, il doit s'agir de l'un des éléments suivants, à condition que les moyens ou toute combinaison de moyens garantissent un niveau de confiance très élevé quant à l'identité du destinataire authentifié:

a) un mécanisme d'authentification à plusieurs facteurs;

b) le portefeuille européen d'identité numérique ou un moyen d'identification électronique notifié qui satisfait aux exigences énoncées à l'article 8 du règlement (UE) nº 910/2014 [i.1] en ce qui concerne le niveau de garantie «élevé» ou «substantiel»;

c) un certificat de signature électronique qualifiée ou de cachet électronique qualifié;

d) d'autres moyens garantissant l'authentification du destinataire identifié. La conformité de l'établissement du lien est confirmée par un organisme d'évaluation de la conformité. Exemple: cela peut inclure l'utilisation de l'un des moyens visés aux points a) à c) ci-dessus pour enregistrer un certificat de client TLS (Transport Layer Security) afin de procéder à des envois automatisés par TLS mutuelle ou pour enregistrer un certificat de cachet numérique afin d'apposer un cachet sur des assertions d'authentification auprès de l'ERDS. D'autres mécanismes dans lesquels les expéditeurs identifiés ont recours à des services tiers délégués peuvent également être appliqués.

— REQ-QERDS-5.2.2-04 [CONDITIONNEL]: si l'expéditeur se connecte au QERDS sur une connexion sécurisée qui nécessite une authentification mutuelle de machine à machine entre la machine de l'expéditeur et le serveur du QERDS fondée sur des certificats délivrés selon la politique de certification normalisée telle que définie dans l'ETSI EN 319 411-1 [2], une fois cette connexion sécurisée établie, des mécanismes d'authentification à facteur unique peuvent être adoptés pour une deuxième phase d'authentification de l'expéditeur si les procédures organisationnelles et les mesures de sécurité mises en place garantissent la confiance dans l'authentification de l'expéditeur.

7) 5.4.1 Dispositions communes

— REQ-ERDS-5.4.1-06: l'ERDS doit générer et mettre à la disposition des parties intéressées légitimes les preuves relatives aux événements liés aux envois électroniques recommandés tels que définis au paragraphe 6 de l'ETSI EN 319 522-1 [3].

— REQ-ERDS-5.4.1-07: l'ERDSP doit archiver les preuves et/ou les résumés de preuves relatifs à toutes les preuves qu'il a émises.

— REQ-ERDS-5.4.1-08: les preuves de l'ERDS générées par l'ERDS doivent respecter la sémantique des preuves définie au paragraphe 8 de l'ETSI EN 319 522-2 [4].

8) 7.2.1 Dispositions communes

— REQ-ERDS-7.2.1-02: le personnel de l'ERDSP intervenant dans des rôles de confiance doit 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.

— REQ-ERDS-7.2.1-03: la conformité au REQ-ERDS-7.2.1-02 doit impliquer des mises à jour régulières (au moins tous les 12 mois) portant sur les nouvelles menaces et les pratiques actuelles en matière de sécurité.

9) 7.3.2 Traitement des supports

— REQ-ERDS-7.3.1-02: toutes les exigences de l'ETSI EN 319 401 [1], paragraphe 7.3.3, s'appliquent.

10) 7.5 Contrôles cryptographiques

— REQ-ERDS-7.5-01A: l'ERDS doit sélectionner et utiliser des techniques cryptographiques appropriées conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [5].

— REQ-ERDSP-7.5-03: la clé de signature privée de l'ERDS est 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 [6] ou dans les critères communs pour l'évaluation de la sécurité des technologies de l'information, version CC:2002, 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) au schéma européen commun de certification de cybersécurité fondé sur des critères communs (EUCC) [7] [8] et certifié au niveau EAL 4 ou supérieur; ou

c) jusqu'au 31.12.2030, à la norme FIPS PUB 140-3 [9] 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 [7] [8], ce dispositif doit être configuré et utilisé conformément à cette certification.

11) 7.8 Sécurité du réseau

— REQ-ERDSP-7.8-04: l'ERDSP doit utiliser des protocoles et algorithmes de pointe pour le chiffrement au niveau de la couche de transport, conformément aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [5].

— REQ-ERDSP-7.8-06: 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.

— REQ-ERDSP-7.8-07: 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.

— REQ-ERDSP-7.8-08: les pare-feu doivent être configurés de manière à empêcher tous les protocoles et accès non nécessaires au fonctionnement du prestataire de services de confiance.

12) 7.12 Plans d'arrêt d'activité de l'ERDSP et de l'ERDS

— REQ-ERDS-7.12-03: le plan d'arrêt d'activité de l'ERDSP 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].

13) 7.14 Chaîne d'approvisionnement

— REQ-ERDS-7.14-01: les exigences spécifiées dans l'ETSI EN 319 401 [1], paragraphe 7.14, s'appliquent.

ANNEXE II

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

Les normes ETSI EN 319 522-1 V1.2.1 (2024-01) («ETSI EN 319 522-1»), ETSI EN 319 522-2 V1.2.1 (2024-01) («ETSI EN 319 522-2»), ETSI EN 319 522-3 V1.2.1 (2024-01) («ETSI EN 319 522-3»), ETSI EN 319 522-4-1 V1.2.1 (2019-01) («ETSI EN 319 522-4-1»), ETSI EN 319 522-4-2 V1.1.1 (2018-09) («ETSI EN 319 522-4-2») et ETSI EN 319 522-4-3 V1.1.1 (2018-09) («ETSI EN 319 522-4-3») s'appliquent.