Journal officiel
de l'Union européenne

FR
Série L

2025/2531

17.12.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/2531 DE LA COMMISSION

du 16 décembre 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 et les spécifications applicables aux registres 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 45 *terdecies*, paragraphe 3,

considérant ce qui suit:

(1) Le règlement (UE) 2024/1183 du Parlement européen et du Conseil [2] a introduit dans le règlement (UE) nº 910/2014 une liste de nouveaux services de confiance et services de confiance qualifiés, y compris l'enregistrement de données électroniques dans un registre électronique qualifié. La Commission doit établir une liste de normes de référence et, si nécessaire, des spécifications applicables à ces services.

(2) Un registre électronique est une séquence d'enregistrements de données électroniques qui doit garantir l'intégrité de ces enregistrements et l'exactitude de leur classement chronologique. Il est nécessaire d'établir un ensemble commun de spécifications pour l'enregistrement des données électroniques dans un registre électronique qualifié pour faire en sorte que cet enregistrement soit effectué de manière chronologique, cohérente et fiable.

(3) La présomption de conformité prévue à l'article 45 *terdecies*, paragraphe 2, du règlement (UE) nº 910/2014 ne devrait s'appliquer que lorsque les services de confiance qualifiés pour l'enregistrement des données électroniques dans un registre électronique qualifié 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.

(4) 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.

(5) La Commission évalue régulièrement de nouvelles technologies, pratiques, normes ou spécifications techniques. Conformément au considérant 75 du règlement (UE) 2024/1183, 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, les pratiques 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, compte tenu également des lignes directrices de février 2025 du Comité européen de la protection des données sur le traitement de données à caractère personnel au moyen de technologies des chaînes de blocs ([5]).

(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 ([6]) et a rendu son avis le 21 octobre 2025 ([7]).

(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 de référence et spécifications

Les normes de référence et les spécifications applicables aux registres électroniques qualifiés, mentionnées à l'article 45 *terdecies*, paragraphe 3, du règlement (UE) n° 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 16 décembre 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]) edpb_guidelines_202502_blockchain_en.pdf.

([6]) 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).

([7]) EDPS Formal comments on the draft Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic ledgers.

ANNEXE

Liste des spécifications techniques et des normes de référence applicables aux registres électroniques distribués qualifiés

1. Aux fins du présent règlement, on entend par:

   a) «immuabilité»: l'état dans lequel se trouve un enregistrement de données d'un registre électronique lorsqu'il est devenu irréversible et ne peut être ni modifié ni supprimé;

   b) «registre électronique distribué»: un registre électronique partagé entre un ensemble de nœuds de registre électronique distribué synchronisés entre eux par un mécanisme de consensus;

   c) «nœud de registre électronique distribué»: un dispositif ou un processus qui fait partie d'un réseau de registre électronique distribué et qui détient une copie complète ou partielle des enregistrements de données d'un registre électronique;

   d) «réseau de registre électronique distribué»: un réseau de nœuds de registre électronique distribué qui constitue un système de registre électronique distribué;

   e) «système de registre électronique distribué», un système qui met en œuvre un registre électronique distribué;

   f) «consensus»: un accord entre les nœuds de registre électronique distribué concernant la validité des transactions et le maintien d'un ensemble cohérent et ordonné de transactions validées dans l'ensemble du système de registre électronique distribué;

   g) «mécanisme de consensus»: l'ensemble des règles et procédures permettant de parvenir à un consensus;

   h) «règles»: l'ensemble des protocoles, des politiques et des mécanismes qui régissent le fonctionnement du système de registre électronique distribué, la manière dont les données sont validées et ajoutées à un registre électronique et la manière dont les participants interagissent;

   i) «transaction»: la plus petite unité d'un processus de travail au sein d'un registre électronique;

   j) «processus de travail»: une ou plusieurs séquences d'actions nécessaires pour produire un résultat conforme aux règles régissant un registre électronique;

   k) «transaction validée»: une transaction pour laquelle l'intégrité, l'authenticité et les conditions spécifiques au protocole requises ont été vérifiées conformément aux règles régissant le système de registre électronique distribué;

   l) «lien cryptographique»: une référence à des données qui est établie à l'aide de techniques cryptographiques appropriées pour garantir l'intégrité, l'authenticité ou la traçabilité des données référencées et la séquence correcte d'enregistrements de données;

   m) «rapport du registre»: une présentation structurée d'informations vérifiables extraites des enregistrements de données d'un registre électronique et fournissant des informations sur des activités données, des états ou le respect de règles prédéfinies;

   n) «fournisseur de registre électronique qualifié»: un prestataire de services de confiance qualifié qui fournit un service de confiance qualifié consistant à enregistrer des données dans un registre électronique qualifié;

   o) «registre électronique distribué qualifié»: un registre électronique distribué qui satisfait aux exigences d'un registre électronique qualifié.

2. Lorsque le prestataire de services de confiance qualifié doit produire un rapport de registre, celui-ci est produit de manière automatisée.

3. Les fournisseurs de registres électroniques qualifiés créent un registre électronique qualifié, enregistrent des données électroniques dans ce registre, l'actualisent et le tiennent à jour conformément aux spécifications établies dans:

   a) pour tous les fournisseurs de registres électroniques qualifiés, ETSI EN 319 401 v3.1.1 (2024-06) avec les adaptations suivantes:

      — 2.1 Références normatives

        [1] 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).

[2] RFC 7515 de l'IETF (mai 2015): «Signatures web JSON (JWS)».

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

[4] Règlement d'exécution (UE) 2024/482 de la Commission du 31 janvier 2024 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).

[5] Règlement d'exécution (UE) 2024/3144 de la Commission du 18 décembre 2024 modifiant le règlement d'exécution (UE) 2024/482 en ce qui concerne les normes internationales applicables et rectifiant ledit règlement d'exécution.

[6] 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».

— 6.1 Énoncé de pratique de service de confiance:

  — REQ-6.1-12 L'énoncé de pratique de registre électronique comprend au moins les informations suivantes:

    — les capacités fonctionnelles et techniques de la plateforme de registre électronique et son utilisation tout au long de la fourniture de l'enregistrement de données dans un registre électronique qualifié en tant que service de confiance qualifié,

    — les mécanismes spécifiques d'authentification de l'origine des données utilisés lors de la fourniture du service,

    — les mécanismes spécifiques de classement chronologique séquentiel utilisés lors de la fourniture du service,

    — le cas échéant, le lien cryptographique utilisé pour assurer la séquence des enregistrements de données,

    — le cas échéant, le mécanisme de consensus garantissant l'immuabilité et l'intégrité des enregistrements de données et des transactions stockés dans le registre, y compris tout délai de précaution supplémentaire requis pour faire en sorte que l'immuabilité et l'intégrité soient atteintes,

    — les mécanismes spécifiques d'intégrité des données utilisés lors de la fourniture du service.

  — 6.2 Modalités et conditions:

    — REQ-6.2-03 Les abonnés et les parties utilisatrices du service de confiance reçoivent individuellement des informations claires, complètes et facilement accessibles, dans un espace accessible au public, relatives aux modalités et conditions précises, y compris les éléments énumérés ci-dessus, avant de nouer une relation contractuelle.

  — 6.3 Politique en matière de sécurité de l'information:

    — REQ-6.3-04X Le prestataire de services de confiance établit des procédures pour notifier à l'organe de contrôle toute modification apportée à la fourniture du service de confiance, conformément aux exigences opérationnelles et aux dispositions législatives et réglementaires applicables. Le prestataire de services de confiance adresse une notification à l'organe de contrôle au moins:

      — un mois avant la mise en œuvre de toute modification,

      — trois mois avant la cessation prévue de la fourniture de services de confiance.

  — 7.2 Ressources humaines:

    — REQ-7.2-04X Le personnel du prestataire de services de confiance 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-7.2-05X Cela implique des mises à jour régulières (au moins tous les 12 mois) sur les nouvelles menaces et les pratiques actuelles en matière de sécurité.

— 7.5 Contrôles cryptographiques:

— REQ-7.5-01X Des contrôles de sécurité appropriés sont mis en place pour la gestion de toutes les clés cryptographiques, de tous les algorithmes cryptographiques et de tous les dispositifs cryptographiques tout au long de leur cycle de vie, en adoptant, le cas échéant, une approche d'agilité cryptographique.

— REQ-7.5-02 Aux fins de la fourniture de ses services de confiance, le prestataire de services de confiance 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 [1].

En particulier:

— REQ-7.5-03 Les fournisseurs de registres électroniques qualifiés établissent l'origine des enregistrements de données dans le registre électronique. À cet égard, ils utilisent des signatures électroniques avancées fondées sur des certificats qualifiés ou des cachets électroniques avancés fondés sur des certificats qualifiés créés par les utilisateurs du service conformément aux normes et spécifications suivantes:

a) ETSI EN 319 122-1 V1.3.1 (2023-06); «Signatures électroniques et infrastructures de confiance (ESI) — Signatures numériques au format CAdES — Partie 1: blocs de construction et signatures au format de base CAdES».

b) ETSI EN 319 132-1 V1.3.1 (2024-07); «Signatures électroniques et infrastructures (ESI) — Signatures numériques au format XAdES — Partie 1: blocs de construction et signatures au format de base XAdES».

c) ETSI TS 119 182-1 V1.2.1 (2024-07). «Signatures électroniques et infrastructures (ESI) — Signatures numériques au format JAdES — Partie 1: blocs de construction et signatures au format de base JAdES», moyennant l'adaptation suivante:

— 5.1.8 Le paramètre d'en-tête x5c (Chaîne de certificat X.509)

— Le paramètre d'en-tête x5c tel que défini dans la clause 4.1.6 de la RFC 7515 de l'IETF [2] doit être présent dans la signature au format JAdES, sous la forme d'un paramètre d'en-tête signé ou non signé.

— La sémantique du paramètre d'en-tête x5c est celle qui est définie dans la clause 4.1.6 de la RFC 7515 [2] de l'IETF.

— La syntaxe du paramètre d'en-tête x5c est celle qui est définie dans la clause 4.1.6 de la RFC 7515 [2] de l'IETF.

— REQ-7.5-04 Les fournisseurs de registres électroniques qualifiés garantissent le classement chronologique séquentiel unique des enregistrements de données dans le registre électronique. À cet égard, ils utilisent des liens cryptographiques, basés sur des tables ou des arbres de hachage, utilisant des fonctions de hachage cryptographique, conformément aux spécifications et normes suivantes:

a) SHA-256 ou taille de sortie supérieure, conformément aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [1].

b) SHA3-256 ou taille de sortie supérieure, conformément aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [1].

À défaut, lorsqu'ils utilisent l'enregistrement du temps pour garantir le classement chronologique séquentiel unique des enregistrements de données dans le registre électronique, les fournisseurs de registres électroniques qualifiés utilisent des horodatages qualifiés.

— REQ-7.5-05 Les fournisseurs de registres électroniques qualifiés garantissent l'intégrité des enregistrements de données enregistrés dans un registre électronique qualifié. À cet égard, ils utilisent des signatures électroniques avancées fondées sur des certificats qualifiés ou des cachets électroniques avancés fondés sur des certificats qualifiés, conformément aux normes et spécifications suivantes:

  a) tout format de signature ou de cachet conforme aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [1];

  b) SHA-256 ou taille de sortie supérieure, conformément aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [1];

  c) SHA3-256 ou taille de sortie supérieure, conformément aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [1];

  d) Les fournisseurs de registres électroniques qualifiés font en sorte que toute modification ultérieure des données enregistrées dans le registre électronique puisse être immédiatement détectée.

— REQ-7.5-06 Si des mécanismes de signature numérique sont utilisés, les clés de signature privées du fournisseur de registre électronique qualifié sont stockées et utilisées 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 ([1]) [6] 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) au schéma européen commun de certification de cybersécurité fondé sur des critères communs (EUCC) ([2]) ([3]) [4] [5] et certifié au niveau EAL 4 ou supérieur; ou

  c) jusqu'au 31.12.2030, à la norme FIPS PUB 140-3 ([4]) [3] niveau 3.

Cette certification est 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 [4] [5], ce dispositif est configuré et utilisé conformément à cette certification.

([1]) 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]) Règlement d'exécution (UE) 2024/482 de la Commission du 31 janvier 2024 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) (JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/2025-01-08).

([3]) Règlement d'exécution (UE) 2024/3144 de la Commission du 18 décembre 2024 modifiant le règlement d'exécution (UE) 2024/482 en ce qui concerne les normes internationales applicables et rectifiant ledit règlement d'exécution (JO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

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

— 7.8 Sécurité du réseau:

— REQ-7.8-14X L'analyse de vulnérabilité requise en vertu du REQ-7.8-13 est effectuée au moins une fois par trimestre.

— REQ-7.8-18X Le test d'intrusion requis en vertu du REQ-7.8-17X est effectué au moins une fois par an.

— REQ-7.8-21X Les pare-feu sont configurés de manière à empêcher tous les protocoles et accès non nécessaires au fonctionnement du prestataire de service de confiance.

— 7.9.1 Surveillance et journalisation:

— REQ-7.9.1-02X Les activités de surveillance tiennent compte de la sensibilité de toute information collectée ou analysée.

— 7.12 Cessation d'activité et plans de cessation du prestataire de services de confiance:

— REQ-7.12-02A Le plan de cessation d'activité du prestataire de services de confiance satisfait 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].

b) En outre, pour tous les fournisseurs de registres électroniques qualifiés utilisant les technologies de registre électronique distribué:

1) ISO 23257: 2022 Technologies des chaînes de blocs et technologies de registre distribué — Architecture de référence, clause 9, fournissant une description complète du système de technologie de registre électronique distribué, du réseau de technologie de registre électronique distribué et des nœuds de technologie de registre électronique distribué correspondants.

2) ISO 23635:2022. Blockchain and distributed ledger technologies — Guidelines for governance, with respect to written and publicly accessible policies and practices related to the governance structure for the electronic ledger service they provide (en anglais).