Journal officiel
de l'Union européenne

FR
Série L

2025/1929

30.9.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/1929 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 l'établissement du lien entre la date et l'heure et les données ainsi que la détermination de l'exactitude des horloges pour la fourniture d'horodatages 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 42, paragraphe 2,

considérant ce qui suit:

(1) Les horodatages électroniques 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. En établissant un lien entre les informations relatives à la date et à l'heure et les données électroniques, les horodatages électroniques qualifiés contribuent à garantir l'exactitude de la date et de l'heure qu'ils indiquent et l'intégrité des documents numériques auxquels la date et l'heure sont associées.

(2) La présomption de conformité prévue à l'article 42, paragraphe 1 *bis*, du règlement (UE) nº 910/2014 ne devrait s'appliquer que lorsque les services de confiance qualifiés de délivrance d'horodatages 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 de l'établissement du lien entre la date et l'heure et les données et de la détermination de l'exactitude des horloges.

(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 d'exécution, 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.

(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.

([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).

([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.

(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) n° 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Les normes de référence et les spécifications mentionnées à l'article 42, paragraphe 2, du règlement (UE) n° 910/2014 figurent à l'annexe du présent règlement.

Article 2

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

([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 les services d'horodatage qualifiés

Les normes ETSI EN 319 421 V1.3.1 ([1]) («ETSI EN 319 421») et ETSI EN 319 422 V1.1.1 ([2]) («ETSI EN 319 422») s'appliquent moyennant les adaptations suivantes:

1. Pour ETSI EN 319 421

   1) 2.1 Références normatives

      — [3] 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».

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

      — [5] ETSI EN 319 422 V1.1.1 (2016-03) «Signatures électroniques et infrastructures (ESI) — Protocole d'horodatage et profils de jetons d'horodatage».

      — [6] vide.

      — [9] 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]).

      — [10] 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) ([4]).

      — [11] 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 ([5]).

   2) 3.1 Termes

      — Période de validité du certificat: intervalle de temps compris entre *notBefore* et *notAfter* inclus, pendant lequel l'autorité de certification (CA) garantit qu'elle conservera des informations sur le statut du certificat.

   3) 3.3 Abréviations

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

   4) 6.2 Déclaration de méthode de service de confiance

      — OVR-6.2-03 Il convient que l'autorité d'horodatage (TSA) indique la disponibilité de son service dans sa déclaration de divulgation d'horodatage.

   5) 7.3 Sécurité du personnel

      — OVR-7.3-02 Le personnel de la TSA intervenant dans des rôles de confiance et, le cas échéant, ses 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-7.3-03 La conformité au point OVR-7.3-02 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.

([1]) EN 319 421 — Signatures électroniques et infrastructures (ESI) — Exigences de politique et de sécurité applicables aux prestataires de service de confiance délivrant des horodatages, V1.3.1.
([2]) EN 319 422 — Signatures électroniques et infrastructures (ESI) - Protocole d'horodatage et profils de jetons d'horodatage, V1.1.1 (2016-03), https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([4]) JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([5]) JO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

6) 7.6.2 Génération de clé de TSU

— TIS-7.6.2-03 La génération de la ou des clés de TSU doit être effectuée 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 [3] 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 [10] [11], et certifié au niveau EAL 4 ou supérieur; ou

c) jusqu'au 31.12.2030, à la norme FIPS PUB 140-3 [7] 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 [10] [11], ce dispositif doit être configuré et utilisé conformément à cette certification.

— TIS-7.6.2-04: vide.

— NOTE 3: vide.

— TIS-7.6.2-05A Il convient que l'algorithme de génération de clés de TSU, la longueur de la clé de signature obtenue et l'algorithme de signature utilisés respectivement pour signer les horodatages et pour signer les certificats de clé publique de TSU, soient conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité [9] et publiés par l'ENISA.

— NOTE 4: vide.

— TIS-7.6.2-06 Toute exportation ou importation de la clé de signature de TSU 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) 7.6.3 Protection de clés privées de TSU

— TIS-7.6.3-02 La clé privée de la TSU 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 [3] 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) [10] [11] et certifié au niveau EAL 4 ou supérieur; ou

c) jusqu'au 31.12.2030, à la norme FIPS PUB 140-3 [7] 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 [10] [11], ce dispositif doit être configuré et utilisé conformément à cette certification.

— TIS-7.6.3-03: vide.

— NOTE 2: vide.

8) 7.6.7 Fin du cycle de vie d'une clé de TSU

— TIS-7.6.7-03A La date d'expiration des clés privées de TSU doit être conforme aux mécanismes cryptographiques agréés [9].

— NOTE 1: vide.

9) 7.10 Sécurité du réseau

— OVR-7.10-05 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-7.10-06 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-7.10-07 Les pare-feu doivent être configurés de manière à empêcher tous les protocoles et accès non nécessaires au fonctionnement de la TSA.

10) 7.14 Cessation de l'autorité d'horodatage et plans de cessation

— OVR-7.14-01A Le plan de cessation 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.4].

2. Pour ETSI EN 319 422

1) 2.1 Références normatives

— [5] vide.

— [6] vide.

— [8] Groupe européen de certification de cybersécurité, sous-groupe sur la cryptographie: «Agreed Cryptographic Mechanisms».

— [9] RFC 9110 HTTP Semantics.

2) 4.1.3 Algorithmes de hachage à utiliser

— La clause suivante doit s'appliquer:

les algorithmes de hachage utilisés pour hacher les informations à horodater, la durée de vie prévue de l'horodatage et les fonctions de hachage sélectionnées par rapport au temps doivent être conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [8].

— NOTE vide.

3) 4.2.3 Algorithmes à prendre en charge

— La clause suivante est applicable:

les algorithmes de signature des jetons d'horodatage à prendre en charge doivent être conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [8].

— NOTE vide.

4) 4.2.4 Longueurs de clé à prendre en charge

— La clause suivante doit s'appliquer:

les longueurs de clé d'algorithme de signature pour l'algorithme de signature choisi doivent être conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA.

— NOTE vide.

5) 5.1.3 Algorithmes à prendre en charge

— La clause suivante doit s'appliquer:

il convient que les algorithmes de hachage pour les données d'horodatage à prendre en charge, la durée de vie prévue de l'horodatage et les fonctions de hachage sélectionnées par rapport au temps soient conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [8].

— NOTE vide.

6) 5.2.3 Algorithmes à utiliser

— La clause suivante doit s'appliquer:

il convient que les algorithmes de hachage utilisés pour hacher les informations à horodater et les algorithmes de signature des jetons d'horodatage soient conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [8].

— NOTE vide.

7) 6.3 Exigences en matière de longueurs de clés

— La clause suivante doit s'appliquer:

la longueur de clé pour l'algorithme de signature de certificat de TSU choisi doit être conforme aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [8].

— NOTE vide.

8) 6.5 Exigences en matière d'algorithme

— La clause suivante doit s'appliquer:

la clé publique de TSU et la signature de certificat de TSU doivent utiliser les algorithmes conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [8].

— NOTE vide.

9) 7 Profils pour les protocoles de transport à prendre en charge

— il convient que le client d'horodatage et le serveur d'horodatage prennent en charge le protocole d'horodatage via HTTPS [9], tel que défini dans la clause 3.4 de la RFC 3161 de l'IETF [1].

10) 8 Identifiants d'objet des algorithmes cryptographiques

— La clause suivante est applicable:

il convient que la clé publique de TSU et la signature de certificat de TSU utilisent des algorithmes conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [8].

11) 9.1 Déclaration de conformité au règlement

— Si la TSA déclare qu'un jeton à horodatage est un horodatage électronique qualifié conformément au règlement (UE) nº 910/2014 [i.2], il doit contenir une instance de l'extension *qcStatements* dans le champ «extension» du jeton d'horodatage, en utilisant la syntaxe définie dans la clause 3.2.6 de la RFC 3739 [i.3].

— L'extension *qcStatements* doit contenir une instance de la mention «*esi4-qtstStatement-1*» telle que définie à l'annexe B.

— L'extension *qcStatements* ne doit pas être marquée comme critique.