Journal officiel
de l'Union européenne

FR
Série L

2025/1566

30.7.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/1566 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 les normes de référence applicables à la vérification de l'identité et des attributs de la personne à laquelle le certificat qualifié ou l'attestation électronique d'attributs qualifiée doit être délivré

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 24, paragraphe 1 *quater*,

considérant ce qui suit:

(1) L'article 24 du règlement (UE) nº 910/2014 exige que les prestataires de services de confiance qualifiés vérifient l'identité et, s'il y a lieu, tous les attributs spécifiques d'une personne physique ou morale à laquelle ils délivrent un certificat qualifié ou une attestation électronique d'attributs qualifiée.

(2) Afin de garantir l'égalité de traitement et la capacité à faire confiance au résultat du processus de vérification, les vérifications devraient être effectuées de manière équivalente par tous les prestataires de services de confiance qualifiés lorsqu'ils délivrent un certificat qualifié ou une attestation électronique d'attributs qualifiée. Conformément aux objectifs du règlement (UE) nº 910/2014, un certain nombre de normes ont été sélectionnées pour satisfaire à ces exigences spécifiques. 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, tout en facilitant l'interopérabilité transfrontière et le bon fonctionnement du marché intérieur.

(3) Il convient de prévoir une période transitoire adéquate pour permettre aux prestataires de services de confiance qualifiés de se conformer aux exigences du règlement (UE) nº 910/2014. Afin de garantir un délai suffisant pour l'audit des prestataires de services de confiance en ce qui concerne le respect des exigences du présent règlement, celui-ci devrait s'appliquer à partir de 24 mois à compter de son entrée en vigueur.

(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.

(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 visées à l'article 24, paragraphe 1 *quater*, 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*.

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

([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

Norme de référence pour la vérification de l'identité et des attributs des personnes auxquelles un certificat qualifié ou une attestation électronique d'attributs qualifiée doit être délivré

La norme ETSI TS 119 461 V2.1.1 (2025-02) s'applique aux fins de la conformité avec l'annexe C, clause C.3, 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».

2) C.3 Cas d'utilisation pour la délivrance de certificats qualifiés ou d'attestations électroniques d'attributs qualifiées conformément à l'article 24, paragraphes 1, 1 *bis* et 1 *ter*, du règlement (UE) nº 910/2014

— [CONDITIONNEL] QTS-C3-01: Si la vérification de l'identité pour un certificat qualifié ou une attestation électronique qualifiée est effectuée conjointement avec la vérification de l'identité afin de délivrer des preuves faisant autorité, ce processus de vérification de l'identité doit:

— avoir fait l'objet d'une évaluation par les pairs ou avoir été certifié par un organisme d'évaluation de la conformité accrédité pour être conforme au niveau de garantie élevé en vertu du règlement (UE) nº 910/2014, ou

— être conforme aux exigences énoncées dans les clauses C3.1 à C3.6.

3) C.3.4 Cas d'utilisation pour la vérification de l'identité par d'autres moyens d'identification

— QTS-C.3.4-06A: L'organisme indépendant d'évaluation de la conformité visé au point [CONDITIONNEL] QTS-C.3.4-06, point c), est accrédité conformément à l'article 3, paragraphe 18, du règlement (UE) nº 910/2014 et, si toutes les exigences applicables sont remplies, l'évaluation doit aboutir à un certificat de conformité fondé sur un audit de certification. Ce processus formel de certification repose sur un processus d'évaluation de la sécurité qui fait référence aux niveaux de garantie définis pour les moyens d'identification électronique notifiés ou les portefeuilles européens d'identité numérique certifiés au titre du règlement (UE) nº 910/2014 et comprend des essais rigoureux visant à évaluer la résistance aux menaces potentielles pour la sécurité. Ces évaluations utilisent des normes techniques pertinentes pour démontrer la capacité de résistance à ce type d'attaques.

4) 9.2.3.4 Cas d'utilisation pour un fonctionnement automatisé

— USE-9.2.3.4-04: l'IPSP établit des valeurs cibles pour les FAR et les FRR, sur la base d'une analyse des risques et de sa procédure en matière de renseignement sur les menaces, en suivant la méthode établie dans le rapport de l'ENISA intitulé «Methodology for sectoral cybersecurity assessments» [i.28] ou une méthode équivalente, dans le cadre de processus entièrement automatisés de vérification de l'identité. Ces valeurs cibles sont égales ou inférieures à celles fixées pour les cas d'utilisation hybrides, lorsque ces derniers existent. L'IPSP maintient ces valeurs cibles pour les FAR et les FRR de manière cohérente, sur la base d'une analyse des risques et de sa procédure en matière de renseignement sur les menaces.

5) 8.3.3 Validation du document d'identité physique

— VAL-8.3.3-21: les tests concernant l'efficacité des mesures relatives à la conformité aux exigences VAL-8.3.3-05X, VAL-8.3.3-05A, VAL-8.3.3-05B, VAL-8.3.3-05C, VAL-8.3.3-07A et VAL-8.3.3-07X sont effectués par un laboratoire accrédité ou une autorité nationale compétente, lorsque ceux-ci sont désignés, au plus tard le 19 août 2027 et sont ensuite renouvelés tous les deux ans.

6) 7.12. Arrêt d'activité et plans d'arrêt d'activité

— OVR-7.12-02: le plan d'arrêt d'activité 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].