EXPOSÉ DES MOTIFS

Les évolutions au niveau du droit européen ont rendu nécessaire une adaptation du texte de loi. Aussi, le retrait des personnes morales du champ d'application du portefeuille d'identité numérique en vue d'un « business wallet » dédié aux personnes morales a donné lieu à des adaptations. À cette occasion, certains passages ont également été remaniés dans un souci de clarté et de précision.

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Digitalisation

Amendements gouvernementaux au projet de loi relative à la mise en place du portefeuille européen d'identité numérique et portant mise en œuvre du règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique et modifiant la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques

TEXTE DES AMENDEMENTS

Amendement 1 concernant l'article 2

(1) À l'article 2 du projet de loi sont apportés les modifications suivantes :

1° le paragraphe 2 est supprimé ;
2° le paragraphe 3 devient le nouveau paragraphe 2 ;
3° le paragraphe 4 devient le nouveau paragraphe 3 ;
4° le paragraphe 5 devient le nouveau paragraphe 4 ;
5° le paragraphe 6 devient le nouveau paragraphe 5 ;
6° le paragraphe 7 devient le nouveau paragraphe 6 ;
7° le paragraphe 8 devient le nouveau paragraphe 7 ;
8° il est inséré un nouveau paragraphe 8 libellé comme suit :

« Le traitement des données à caractère personnel par les autorités compétentes surnommées est autorisé dans la mesure où cela est nécessaire pour garantir le bon fonctionnement et l'intégrité du portefeuille, ainsi que pour la fourniture des services liés au portefeuille. ».

(2) À l'article 2, paragraphe 1, du projet de loi, après les termes « l'article 5*bis*, paragraphe 1er » est inséré le signe de ponctuation « , ».

(3) À l'article 2, paragraphe 2, du projet de loi, après les termes « à l'article 46*bis*, paragraphe 1er » est inséré le signe de ponctuation « , ».

(4) À l'article 2, paragraphe 5, devenu le nouveau paragraphe 4, du projet de loi, après les termes « l'article 3, paragraphe 1er » est inséré le signe de ponctuation « , ».

(5) À l'article 2, paragraphe 6, devenu le nouveau paragraphe 5, du projet de loi sont apportés les modifications suivantes :

1° les termes « Commissariat du gouvernement à la protection des données à caractère personnel auprès de l'État » sont remplacés par ceux de « Commissariat du Gouvernement à la souveraineté des données » ;

2° après les termes « l'article 3, paragraphe 3 » est inséré le signe de ponctuation « , » ;

3° après les termes « règlement d'exécution (UE) 2025/848 de la Commission du 6 mai 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne l'enregistrement des parties utilisatrices de portefeuille » sont insérés ceux de « , tel que modifié ».

(6) À l'article 2, paragraphe 7, devenu le nouveau paragraphe 6, du projet de loi, après les termes « l'article 7, paragraphe 1er » est inséré le signe de ponctuation « , ».

(7) À l'article 2, paragraphe 8, devenu le nouveau paragraphe 7, du projet de loi, après les termes « l'article 8, paragraphe 1er » est inséré le signe de ponctuation « , ».

Commentaire de l'amendement

L'amendement de supprimer le paragraphe 2 reflète la possibilité de confier la mission de certification aussi à des prestataires internationaux accrédités à l'étranger.
Le nouveau paragraphe 8 crée une base légale pour les traitements de données nécessaires. La condition de la nécessité impose une limitation stricte, tandis que les éléments de fonctionnement, intégrité et fourniture de service relatives définissent les finalités de ces traitements.

Amendement 2 concernant l'article 3

(1) À l'article 3 du projet de loi sont apportés entre autres les modifications suivantes :

1° les paragraphes 5 et 6 sont supprimés ;
2° le paragraphe 7 devient le nouveau paragraphe 5 ;
3° le paragraphe 8 devient le nouveau paragraphe 6 ;
4° le paragraphe 9 devient le nouveau paragraphe 7 ;
5° le paragraphe 10 devient le nouveau paragraphe 8 ;
6° il est inséré un nouveau paragraphe 9 libellé comme suit :

« Les données d'identification personnelle au sens de l'article 3, point 3), du règlement (UE) n° 910/2014, si vérifiables, font foi de l'identité de la personne concernée et permettent de satisfaire à toute obligation d'identification indépendamment du caractère électronique ou non électronique de la procédure, sauf disposition légale contraire l'excluant expressément. ».

(2) À l'article 3, paragraphe 1, du projet de loi, les termes « et morales » sont biffés, et après les termes « l'article 5*bis*, paragraphe 5, point f) » est inséré le signe de ponctuation « , ».

(3) À l'article 3, paragraphe 2, du projet de loi, le troisième tiret est supprimé.

(4) À l'article 3, paragraphe 3, du projet de loi, après les termes « registre national des personnes physiques » sont insérés ceux de « , à l'exclusion du portrait numérique de l'utilisateur. Le portrait numérique est fourni par le CTIE sur base d'une communication préalable par l'utilisateur des informations nécessaires à cet effet, telles que requises et spécifiées par le CTIE le cas échéant. ».

(5) À l'article 3, paragraphe 4, du projet de loi sont apportés les modifications suivantes :

1° après les termes « l'annexe, point 1, tableau 1 » est inséré le signe de ponctuation « , » ;

2° après les termes « règlement d'exécution (UE) 2024/2977 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les données d'identification personnelles et les attestations électroniques d'attributs délivrés aux portefeuilles européens d'identité numérique, » sont insérés ceux de « tel que modifié, » ;

3° après les termes « les données d'identification personnelle des utilisateurs personnes physiques sont » sont insérés ceux de « le portrait numérique et » ;

4° après les termes « données énumérées à l'article 5, paragraphe 2, lettres a), d) et f) » est inséré le signe de ponctuation « , » ;

5° après les termes « l'article 5*bis*, paragraphe 5, point f) » est inséré le signe de ponctuation « , ».

(6) À l'article 3, paragraphe 7, devenu le nouveau paragraphe 5, du projet de loi, le terme « aux paragraphes » est remplacé par celui de « au paragraphe », et les termes « et 6 » sont biffés.

(7) À l'article 3, paragraphe 9, devenu le nouveau paragraphe 7, première phrase, premier tiret, du projet de loi, sont apportés les modifications suivantes :

1° après les termes « l'article 5*bis*, paragraphe 14 » est inséré le signe de ponctuation « , » ;

2° les termes « numéro personnel administratif » sont remplacés par ceux de « numéro administratif personnel » ;

3° le terme « et » est remplacée par le signe de ponctuation « , » ;

4° après les termes « l'identifiant de son unité de portefeuille » sont insérés ceux de « et son numéro d'identification au sens de l'article 1er de la loi modifiée du 19 juin 2013 précitée. » ;

5° le point-virgule à la fin du tiret est supprimé.

(8) L'article 3, paragraphe 9, devenu le nouveau paragraphe 7, première phrase, deuxième tiret, du projet de loi est supprimé.

(9) L'article 3, paragraphe 9, devenu le nouveau paragraphe 7, deuxième phrase, du projet de loi est remplacée par le libellé suivant :

« Sauf dispositions contraires, les données visées au présent paragraphe sont conservées pour la durée de 5 années après la fin de validité de l'unité de portefeuille pour prévenir tout dysfonctionnement résultant de la réutilisation de données invalidés. ».

Commentaire de l'amendement

L'amendement tient compte de la modification apportée au niveau de l'UE visant à inclure le portrait dans la liste des données d'identification personnelle obligatoires.

Le législateur a fait usage de la marge de manœuvre accordée par le droit européen pour opter en faveur de la possibilité d'une obligation de portrait sans « opt-out » dans une vision de simplification du fonctionnement et de la gestion du portefeuille et afin de s'assurer de l'homogénéité des données dans le PID. En ce qui concerne la communication préalable de l'utilisateur du portrait : En général, le portrait numérique proviendra de la puce des documents de voyage lisibles par machine électronique (DVLM-e) conformes au document 9303 de l'Organisation de l'aviation civile internationale (OACI).

Au paragraphe 9, devenu le nouveau paragraphe 7, un stockage du numéro d'identification national, la « matricule », dans le registre dédié est ajouté pour des raisons d'efficacité, afin de pouvoir facilement réidentifier un utilisateur de portefeuille lors d'une authentification sur des services publics en ligne, sans devoir accéder à chaque fois au RNPP. Tout en plus, une conservation est prévue pour garantir un fonctionnement plus efficace du portefeuille. Par la conservation du numéro administratif personnel, de l'identifiant des données d'identité, de l'unité de portefeuille et de la matricule, il est évité qu'un même ancien identifiant sera assigné une nouvelle fois à un portefeuille différent. Ainsi le risque de confusion d'identité des utilisateurs est minimisé. Les données d'identification personnelles ne sont pas conservés, ni d'autres données supplémentaires.

Le nouveau paragraphe 9 rend explicite l'effet juridique des données d'identification personnelle et le droit de l'utilisateur de s'identifier à l'aide de son portefeuille d'identité numérique même dans un contexte analogue. Pourtant, il faut que l'authenticité du portefeuille soit vérifiable.

Amendement 3 concernant l'article 4

Le dispositif de l'article 4 du projet de loi est remplacé comme suit :

« **Art. 4. Enrôlement de l'utilisateur**

Afin de garantir que les données d'identification personnelle émises vers le portefeuille d'un utilisateur, représentent l'utilisateur de manière univoque, conformément à l'article 5*bis*, paragraphe 5, point f), du règlement (UE) n° 910/2014, ce dernier s'enrôle :

a) soit sur le guichet unique électronique visé à l'article 6 de la loi modifiée du 24 mai 2011 relative aux services dans le marché intérieur :
   - par tout moyen d'identification électronique notifié de niveau de garantie élevé au sens de l'article 8, paragraphe 2, point c), du règlement (UE) n° 910/2014, ou
   - par tout moyen d'identification électronique notifié de niveau de garantie substantiel au sens de l'article 8, paragraphe 2, point b), du règlement (UE) n° 910/2014, combiné avec les procédures d'enrôlement à distance supplémentaires conformes aux exigences établies par l'acte d'exécution (UE) 2026/798 de la Commission du 7 avril 2026 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les normes de référence et les spécifications applicables à l'enrôlement à distance des utilisateurs pour les portefeuilles européens d'identité numérique par des moyens d'identification électronique conformes au niveau de garantie substantiel combinés avec des procédures d'enrôlement à distance

supplémentaires lorsque la combinaison répond aux exigences du niveau de garantie élevé, prévu à l'article 5*bis*, paragraphe 24, du règlement (UE) n° 910/2014 ;

b) soit en s'identifiant à l'aide de sa carte d'identité ou de son passeport auprès de l'administration communale du lieu de résidence de l'utilisateur, auprès d'une mission diplomatique ou consulaire luxembourgeoise établie à l'étranger, ou dans les locaux du guichet physique. »

Commentaire de l'amendement

L'amendement était nécessaire pour permettre à l'utilisateur l'enrôlement depuis l'étranger.

Amendement 4 concernant l'article 5

À l'article 5 du projet de loi sont apportés les modifications suivantes :

1° après les termes « l'article 5*bis*, paragraphe 3 » sont insérés ceux de « , deuxième phrase, » ;

2° les termes « ne peut pas être divulgué » sont remplacés par ceux de « n'est pas divulgué » ;

3° les termes « ou lorsque ceux-ci sont sujets aux droits de propriété intellectuelle » sont remplacés par ceux de « et il peut être dérogé à l'obligation prévue à l'article 5*bis*, paragraphe 3, première phrase, du règlement (UE) n° 910/2014 pour des raisons de coûts économiques disproportionnés ou d'inconvénients opérationnels majeurs ».

Commentaire de l'amendement

Il fut précisé les raisons pour lesquelles le législateur peut avoir recours à des codes sources propriétaires.

Amendement 5 concernant l'article 6

(1) À l'article 6, paragraphes 1er et 2, du projet de loi, après les termes « par tous les moyens » sont insérés ceux de « , dont les délais et modalités pratiques sont fixés dans les conditions d'utilisation du portefeuille », et les phrases « Ce dernier est tenu de révoquer la validité de cette unité de portefeuille endéans les vingt quatre heures de la réception de la demande. » sont supprimées.

(2) À l'article 6, paragraphe 1er , du projet de loi, après les termes « l'article 5*bis*, paragraphe 9, lettre a) » est inséré le signe de ponctuation « , ».

(3) À l'article 6, paragraphe 2, du projet de loi, après les termes « l'article 5*bis*, paragraphe 9, lettre c) » est inséré le signe de ponctuation « , », et les termes « ou de cessation d'activité de la personne morale » sont biffés.

(4) L'article 6, paragraphe 3, du projet de loi est supprimé. Le paragraphe 4 devient le nouveau paragraphe 3.

(5) À l'article 6, paragraphe 4, devenu le nouveau paragraphe 3, du projet de loi, les termes « ou morale » sont biffés.

Commentaire de l'amendement

Des précisions furent apportées au texte afin de clarifier la mise en œuvre de la loi et de laisser au fournisseur la flexibilité nécessaire pour mettre en place et adapter ses propres procédures. Le règlement (UE) n° 910/2014 prévoit la suspension « dans les meilleurs délais ». Une définition normative de cette notion irait à l'encontre de la prééminence d'interprétation de la CJUE. Afin de rendre ce concept juridique vague plus facile à appliquer dans la pratique, il est toutefois recommandé que le CTIE se dote de ses propres recommandations internes. Dans ce contexte, le CTIE pourrait se baser sur la référence de 24 heures visée par l'article 9 du règlement d'exécution (UE) 2025/847 de la Commission du 6 mai 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les réactions aux atteintes à la sécurité des portefeuilles européens d'identité numérique.

Amendement 6 concernant l'article 8

(1) À l'article 8, paragraphe 1er, du projet de loi, le terme « précité » est remplacé par ceux de « de la Commission du 6 mai 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne l'enregistrement des parties utilisatrices de portefeuille, tel que modifié ».

(2) À l'article 8, paragraphe 4, du projet de loi, après les termes « paragraphe 2, points 1° et 3° » est inséré le signe de ponctuation « , ».

Amendement 7 concernant l'article 9

À l'article 9 du projet de loi sont apportés les modifications suivantes :

1° le terme « met » est remplacé par ceux de « est l'organisme chargé de mettre » ;

2° après les termes « règlement d'exécution (UE) 2025/848 » sont insérés ceux de « de la Commission du 6 mai 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne l'enregistrement des parties utilisatrices de portefeuille, tel que modifié » ;

3° après les termes « public en ligne » est inséré le signe de ponctuation « , » ;

4° après les termes « l'article 3, paragraphe 4 » est inséré le signe de ponctuation « , ».

Commentaire de l'amendement

Des clarifications furent apportées au texte.

Amendement 8 concernant l'article 10

À l'article 10, paragraphe 1er, du projet de loi, le terme « procède » est remplacé par ceux de « est l'organisme chargé de procéder ».

Commentaire de l'amendement

Des clarifications furent apportées au texte.

Amendement 9 concernant l'article 11

L'article 11, paragraphe 2, du projet de loi est supprimé.

Commentaire de l'amendement

Les dispositions relatives font partie du droit européen directement applicable.

Amendement 10 concernant l'article 12

À l'article 12 du projet de loi, après les termes « sont opérés », le signe de ponctuation « , » est supprimé.

Amendement 11 concernant l'article 14

Le libellé de l'article 14 du projet de loi est remplacé comme suit :

« Le CTIE est désigné comme organisme du secteur public qui, pour le compte de l'organisme du secteur public responsable de la source authentique concernée peut émettre des attestations électroniques d'attributs, au sens de l'article 3 point 46, et de l'article 45*septies* du règlement (UE) n° 910/2014.

Sous réserve de la mise en place des démarches numériques respectives, pour les fins du traitement de la demande d'un utilisateur d'attestation électronique d'un attribut, le CTIE est autorisé à accéder aux données y nécessaires et à les traiter.
».

Commentaire de l'amendement

Des clarifications furent apportées au texte du premier alinéa en ligne avec la conception de cet alinéa en tant que désignation. Le CTIE a le droit d'émettre des attestations d'attributs pour le compte de chaque responsable pour une source authentique. Le CTIE agit ainsi comme intermédiaire, et, par exemple, l'administration responsable de la source authentique a le choix de se servir du CTIE pour la création d'attestations.

Le nouveau deuxième alinéa renforce la sécurité légale en créant une base légale explicite pour le traitement de données dans le cadre de la demande d'attestation électronique. Le CTIE agit dans ces cas en tant qu'intermédiaire pour le responsable d'une source authentique, qui par son propre choix a confié la mission de délivrance d'attestations électroniques au CTIE. Le CTIE n'intervient donc que si le responsable lui a confié cette mission. Le CTIE n'intervient que sur la demande particulière d'un utilisateur et les données qu'il peut accéder et traiter se limitent strictement aux données particulières nécessaires pour réaliser la demande.

Amendement 12 concernant l'article 15

À l'article 15, paragraphe 2, du projet de loi, les termes « prévue dans tout autre texte de loi similaire » sont biffés.

Amendement 13 concernant l'article 17

À l'article 17, paragraphes 1er et 3, du projet de loi, les termes « a priori et a posteriori » sont remplacés par ceux de « en amont et en aval ».

Amendement 14 concernant l'article 18

À l'article 18, paragraphe 1er, du projet de loi, les termes « a posteriori » sont remplacés par ceux de « en aval ».

Amendement 15 concernant l'article 20

À l'article 20, paragraphe 2, du projet de loi, après les termes « l'article 4, point 12° » est inséré le signe de ponctuation « , ».

Amendement 16 concernant l'article 21

(1) À l'article 21, paragraphe 3, du projet de loi, les termes « Commissariat du gouvernement à la protection des données à caractère personnel auprès de l'État » sont remplacés par ceux de « Commissariat du Gouvernement à la souveraineté des données ».

(2) À l'article 21, paragraphe 4, du projet de loi, le terme « 3ème » est remplacé par celui de « 4ème ».

(3) À l'article 21, paragraphe 5, du projet de loi sont apportés les modifications suivantes :

1° les termes « la 4ème phrase est remplacée » sont remplacés par ceux de « les 5ème, 6ème, et 7ème phrases sont remplacées » ;
2° la phrase « L'élément visé à la lettre a) de l'alinéa qui précède n'est pas activé pour les cartes d'identité délivrées aux majeurs incapables » est supprimée.

(4) À l'article 21 du projet de loi, est inséré un nouveau paragraphe 6 libellé comme suit :

« (6) Après l'article 15, paragraphe 1er, est insérée un nouveau paragraphe 1*bis* comprenant le libellé suivant :

« (1*bis*) La personne réquisitionnée conformément au paragraphe 1er peut satisfaire à l'obligation de présentation de sa carte d'identité en présentant les données d'identification requises au moyen du portefeuille européen d'identité numérique visé par la loi du […] relative à la mise en place du portefeuille européen d'identité numérique et portant mise en œuvre du règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique et modifiant la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques. »

».

Commentaire de l'amendement

Le nouveau paragraphe 6 renforce la sécurité légale en créant une base légale explicite pour l'utilisation du portefeuille au lieu de la carte d'identité physique. L'utilisateur présente alors les données d'identification personnelle ou l'attestation électronique de la carte d'identité en tant qu'attribut sur son portefeuille.

Amendement 17 concernant l'article 22

L'article 22 devient le nouvel article 23.

Il est inséré un nouvel article 22 libellé comme suit :

« **Art. 22 Entrée en vigueur**

L'article 21, paragraphe 4 et paragraphe 5 entrent en vigueur le premier jour du vingt-quatrième mois qui suit celui de la publication de la présente loi au Journal officiel du Grand-Duché de Luxembourg.
».

Commentaire de l'amendement

La fin de la signature électronique par le moyen de la carte d'identité fut reportée pour permettre une période de transition.

Journal officiel
de l'Union européenne

FR
Série L

2025/2527

17.12.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/2527 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 applicables aux certificats qualifiés d'authentification de site internet

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, paragraphe 2,

considérant ce qui suit:

(1) Les certificats qualifiés d'authentification de site internet sont essentiels pour garantir la confiance et la transparence dans les interactions en ligne. Ils permettent d'authentifier un site internet et de relier ce site à la personne physique ou morale à laquelle le certificat est délivré. La Commission doit établir une liste de normes de référence applicables à ces certificats.

(2) Les normes de référence devraient permettre la mise en œuvre de différents types de certificats qualifiés d'authentification de site internet pour différents cas d'utilisation, y compris leur utilisation au titre de la directive (UE) 2015/2366 du Parlement européen et du Conseil ([2]). Elles devraient tenir compte des pratiques établies et être largement reconnues dans les secteurs concernés. Afin de permettre l'innovation et de répondre à divers besoins techniques et opérationnels, les normes de référence devraient également prévoir la faculté de délivrer les certificats qualifiés d'authentification de site internet sous différentes formes, à savoir sous forme de certificats autonomes, de certificats liés à d'autres certificats, ou dans d'autres configurations répondant aux exigences du règlement (UE) nº 910/2014. Cette flexibilité en ce qui concerne la délivrance de certificats qualifiés d'authentification de site internet ménage la possibilité d'adapter les certificats pour répondre aux besoins d'un large éventail de cas d'utilisation qui préservent la confiance et l'interopérabilité entre les États membres, sans porter atteinte à la liberté dont jouissent les fournisseurs de navigateurs internet pour assurer la sécurité du web, l'authentification de domaine et le chiffrement du trafic internet, de la manière et par les moyens technologiques qu'ils jugent les plus appropriés.

(3) Afin de garantir un délai suffisant pour l'audit des prestataires de services de confiance qualifiés en ce qui concerne le respect des exigences du présent règlement, celui-ci devrait s'appliquer à partir de 12 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 ([3]), 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]) Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) nº 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

([3]) 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).

(5) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([4]) et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([5]) s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du présent règlement.

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

(7) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Les normes de référence mentionnées à l'article 45, paragraphe 2, du règlement (UE) nº 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 6 janvier 2027.

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

([4]) 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).

([5]) 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]) 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) nº 45/2001 et la décision nº 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 for qualified certificates for website authentication.

ANNEXE

Liste des normes de référence applicables aux certificats qualifiés d'authentification de site internet

1. Pour les certificats qualifiés d'authentification de site web qui sont délivrés en vue d'une utilisation dans l'authentification de sécurité de la couche «transport» en dehors du cadre d'un navigateur web:

   — ETSI EN 319 411-2 V2.6.1 (2025-06); ces certificats sont délivrés conformément à la politique de certification QNCP-w-gen, à la politique de certification QEVCP-w ou à la politique de certification QNCP-w, telles que spécifiées dans ladite norme, ou

   — ETSI TS 119 495 V1.7.1 (2024-07).

2. Pour les certificats qualifiés d'authentification de site internet autres que ceux visés au point 1, y compris dans le cadre d'un navigateur web:

   — ETSI TS 119 411-5 V2.1.1 (2025-02).

Journal officiel
de l'Union européenne

FR
Série L

2025/2162

28.10.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/2162 DE LA COMMISSION

du 27 octobre 2025

portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne l'accréditation des organismes d'évaluation de la conformité procédant à l'évaluation des prestataires de services de confiance qualifiés et des services de confiance qualifiés qu'ils fournissent, le rapport d'évaluation de la conformité et le système d'évaluation de la conformité

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 20, paragraphe 4,

considérant ce qui suit:

(1) Conformément à l'article 20, paragraphe 1, et à l'article 21, paragraphe 1, du règlement (UE) nº 910/2014, les prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent doivent faire l'objet d'un audit par un organisme d'évaluation de la conformité. Les rapports d'évaluation de la conformité qui en résultent confirment que les exigences énoncées dans ledit règlement et à l'article 21 de la directive (UE) 2022/2555 du Parlement européen et du Conseil ([2]) sont respectées. Par conséquent, il est nécessaire d'établir un cadre harmonisé et solide pour l'accréditation des organismes d'évaluation de la conformité, les systèmes d'évaluation de la conformité qu'ils mettent en œuvre, les évaluations de la conformité qu'ils effectuent conformément à ces systèmes et les rapports d'évaluation de la conformité qui en résultent.

(2) L'accréditation des organismes d'évaluation de la conformité effectuant l'audit des prestataires de services de confiance qualifiés et des services de confiance qualifiés qu'ils fournissent, le rapport d'évaluation de la conformité et le système d'évaluation de la conformité devraient satisfaire aux exigences énoncées dans le présent règlement. Les organismes d'évaluation de la conformité peuvent satisfaire à ces exigences soit de manière indépendante, soit en recourant à la certification composite, soit en sous-traitant à des entités dûment accréditées.

(3) Les organismes d'évaluation de la conformité accrédités pour l'évaluation des prestataires de services de confiance qualifiés et des services de confiance qualifiés qu'ils fournissent en ce qui concerne la délivrance d'attestations électroniques d'attributs qualifiées devraient être autorisés à délivrer le rapport d'évaluation de la conformité requis par l'article 45 *septies*, paragraphe 3, du règlement (UE) nº 910/2014.

(4) Afin de contribuer à la transparence du processus d'accréditation, le certificat d'accréditation délivré à un organisme d'évaluation de la conformité conformément à l'article 5 du règlement (CE) nº 765/2008 du Parlement européen et du Conseil ([3]) devrait contenir suffisamment d'informations pour permettre aux tiers de vérifier que l'organisme d'évaluation de la conformité accrédité est autorisé à procéder à une évaluation de la conformité au titre du règlement (UE) nº 910/2014.

(5) Afin de préserver l'intégrité et l'exactitude des certificats d'accréditation, les organismes nationaux d'accréditation devraient veiller à ce que ces certificats correspondent à des informations à jour.

([1]) JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([3]) Règlement (CE) nº 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) nº 339/93 du Conseil (JO L 218 du 13.8.2008, p. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

(6) Pour garantir l'intégrité du processus d'accréditation, le certificat d'accréditation délivré à un organisme d'évaluation de la conformité peut être suspendu ou retiré à tout moment en ce qui concerne chaque service de confiance qualifié pour l'évaluation duquel l'organisme d'évaluation de la conformité a été accrédité. La suspension ou le retrait peut intervenir après une sanction par l'organisme national d'accréditation ou être effectué volontairement par l'organisme d'évaluation de la conformité lui-même.

(7) Aux fins de l'harmonisation de ce cadre d'accréditation, le présent règlement devrait être fondé sur des normes établies, qui reflètent les pratiques établies et qui sont largement reconnues dans les secteurs concernés.

(8) Afin de renforcer la transparence, les organismes d'évaluation de la conformité devraient rendre publics les certificats de conformité qu'ils délivrent. Les certificats de conformité confirment les décisions de certification positives prises par les organismes d'évaluation de la conformité. Toutefois, seul l'organe de contrôle accorde ou retire le statut qualifié au prestataire de services de confiance et aux services de confiance qu'il fournit.

(9) Pour évaluer la conformité des prestataires de services de confiance qualifiés et des services de confiance qualifiés qu'ils fournissent au règlement (UE) n° 910/2014 et à l'article 21 de la directive (UE) 2022/2555, les organismes d'évaluation de la conformité devraient utiliser un système d'évaluation de la conformité. Les organismes d'évaluation de la conformité devraient utiliser des normes comme critères de référence pour évaluer les prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent, en tenant compte des versions et des adaptations de ces normes figurant dans les actes d'exécution spécifiques au service fondés sur le règlement (UE) n° 910/2014. Ces normes devraient tenir compte des pratiques établies et être largement reconnues dans les secteurs concernés.

(10) Les systèmes d'évaluation de la conformité définissent les règles et procédures que les organismes d'évaluation de la conformité doivent utiliser pour évaluer les prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent. Ces systèmes sont évalués par les organismes nationaux d'accréditation au regard des exigences énoncées dans le présent règlement. Le contenu de ces systèmes est susceptible d'évoluer au fil du temps. Afin de faciliter l'application de versions successives des systèmes d'évaluation de la conformité, les organismes d'évaluation de la conformité accrédités devraient mettre en place un processus spécifique pour gérer les évolutions d'un système pour lequel ils sont accrédités.

(11) Afin de superviser l'élaboration et la maintenance des programmes d'évaluation de la conformité, il convient d'attribuer à chaque système d'évaluation de la conformité un propriétaire du système. Le propriétaire du système peut être un organisme d'évaluation de la conformité, un organisme gouvernemental ou une autorité, une association professionnelle, un groupe d'organismes d'évaluation de la conformité ou tout organisme ou groupe d'organismes approprié, et il peut être différent de l'organisme d'évaluation de la conformité qui gère le système.

(12) Afin d'assurer la continuité de la fourniture des services des organismes d'évaluation de la conformité, l'accréditation de ces derniers devrait rester valable pour les versions antérieures des normes référencées dans le système d'évaluation de la conformité. Dans ces cas, les organismes d'évaluation de la conformité devraient faire explicitement référence à ces versions antérieures des normes, y compris l'année et le numéro de version.

(13) Afin de renforcer la flexibilité, les organismes nationaux d'accréditation devraient être autorisés à proposer une accréditation en portée flexible, permettant aux organismes d'évaluation de la conformité, dans des circonstances particulières, d'ajouter des activités supplémentaires à leur portée d'accréditation sans qu'une évaluation par l'organisme national d'accréditation soit nécessaire. Lors de la conception de l'accréditation en portée flexible, les organismes nationaux d'accréditation envisageront l'accréditation des portées flexibles telle que définie par la coopération européenne pour l'accréditation, désignée conformément au règlement (CE) n° 765/2008. Lorsque les organismes nationaux d'accréditation autorisent les organismes d'évaluation de la conformité à recourir à cette accréditation en portée flexible, ils devraient l'indiquer dans le certificat d'accréditation à des fins de transparence. Afin d'accroître la flexibilité même lorsque les organismes nationaux d'accréditation ne proposent pas d'accréditation en portée flexible, ces organismes devraient examiner attentivement, avant de réévaluer l'organisme d'évaluation de la conformité accrédité, l'incidence des modifications apportées au système d'évaluation de la conformité pour lequel cet organisme a été accrédité.

(14) Afin de garantir la fiabilité des systèmes d'évaluation de la conformité, les propriétaires devraient veiller à ce que leurs systèmes d'évaluation de la conformité ne permettent pas la délivrance de décisions de certification positives, ou d'un éventuel certificat de conformité, lorsque l'évaluation de la conformité met en évidence une quelconque non-conformité aux exigences du règlement (UE) n° 910/2014, ou à l'article 21 de la directive (UE) 2022/2555, en ce qui concerne les prestataires de services de confiance qualifiés et le service de confiance qualifié qu'ils fournissent. En effet, si un rapport d'évaluation de la conformité peut relever des non-conformités et inclure des plans de mesures correctives potentiels, aucun certificat de conformité ou décision de certification positive ne devrait être délivré lorsque des non-conformités sont constatées.

(15) Afin de garantir la transparence de leurs pratiques, les propriétaires de systèmes devraient mettre à la disposition du public un résumé de leurs systèmes d'évaluation de la conformité. Le résumé devrait contenir une description de l'ensemble des règles et procédures suivies pour évaluer la conformité des prestataires de services de confiance qualifiés et des services de confiance qualifiés qu'ils fournissent aux exigences énoncées dans le règlement (UE) nº 910/2014 et à l'article 21 de la directive (UE) 2022/2555.

(16) Afin de contribuer à la qualité, la sécurité et la fiabilité des activités du prestataire de services de confiance qualifié, le rapport d'évaluation de la conformité devrait recenser, le cas échéant, les possibilités d'amélioration susceptibles de perfectionner la manière dont le prestataire de services de confiance qualifié et les services de confiance qualifiés qu'il fournit satisfont aux exigences applicables.

(17) Afin de favoriser la transparence et de faciliter la tâche des organes de contrôle chargés de vérifier qu'un prestataire de services de confiance qualifié évalué et les services de confiance qualifiés qu'il fournit satisfont aux exigences applicables, le rapport d'évaluation de la conformité devrait inclure certaines informations minimales. En particulier, afin de faciliter l'identification des services devant être inscrits sur la liste nationale de confiance conformément à l'article 22 du règlement (UE) nº 910/2014, le cas échéant, il convient de fournir, dans le rapport d'évaluation de la conformité, une description détaillée de la hiérarchie fonctionnelle de l'infrastructure à clé publique, par type de service de confiance qualifié.

(18) Afin de favoriser la transparence et de faciliter la vérification et le contrôle de l'accréditation des organismes d'évaluation de la conformité conformément au règlement (UE) nº 910/2014, les organismes nationaux d'accréditation devraient, le cas échéant, fournir un historique de la portée de l'accréditation, y compris la date de début et, éventuellement, la date de fin de l'accréditation pour chaque service de confiance qualifié.

(19) Afin d'assurer la continuité des organismes d'évaluation de la conformité qui ont déjà été accrédités et de soutenir la transition vers les règles énoncées dans le présent règlement, les organismes d'évaluation de la conformité qui sont actuellement accrédités au titre de la norme ETSI EN 319 403 version 2.2.2, ou d'une version antérieure de celle-ci, ne devraient pas être réaccrédités au titre du règlement (UE) nº 910/2014 avant le 17 mai 2027. Après cette date, les organismes d'évaluation de la conformité devraient être évalués par l'organisme national d'accréditation au regard des exigences énoncées dans le présent règlement.

(20) 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 ([4]), 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.

(21) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([5]) et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([6]) s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du présent règlement.

([4]) 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).

([5]) 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).

([6]) 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).

(22) 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 ([7]) et a rendu son avis le 8 août 2025 ([8]).

(23) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Définitions

Aux fins du présent règlement, on entend par:

1) «propriétaire du système»: une entité ou un groupe d'entités qui est responsable de l'élaboration et de la maintenance d'un système d'évaluation de la conformité;

2) «décision de certification»: une décision de certification qui fait suite à une évaluation de la conformité effectuée par un organisme d'évaluation de la conformité, par laquelle cet organisme confirme ou infirme qu'un prestataire de services de confiance qualifié donné et le service de confiance qualifié qu'il fournit respectent les exigences énoncées dans le règlement (UE) nº 910/2014 et à l'article 21 de la directive (UE) 2022/2555;

3) «certificat de conformité»: un document par lequel un organisme d'évaluation de la conformité atteste une décision de certification qui confirme qu'un prestataire de services de confiance qualifié donné et le service de confiance qualifié qu'il fournit respectent les exigences énoncées dans le règlement (UE) nº 910/2014 et à l'article 21 de la directive (UE) 2022/2555;

4) «système d'évaluation de la conformité»: un ensemble des règles et procédures utilisées par les organismes d'évaluation de la conformité pour évaluer la conformité des prestataires de services de confiance qualifiés et des services de confiance qualifiés qu'ils fournissent aux exigences énoncées dans le règlement (UE) nº 910/2014 et à l'article 21 de la directive (UE) 2022/2555;

5) «rapport d'évaluation de la conformité»: un document qui fournit des informations détaillées, le cas échéant en complément de celles contenues dans une décision de certification et dans le certificat de conformité qui lui est associé, sur la méthode utilisée pour effectuer, conformément à un système d'évaluation de la conformité, une évaluation de la conformité d'un prestataire de services de confiance qualifié donné et du service de confiance qualifié qu'il fournit aux exigences énoncées dans le règlement (UE) nº 910/2014 et à l'article 21 de la directive (UE) 2022/2555, ainsi que sur les résultats de l'évaluation de la conformité;

6) «accréditation»: une accréditation au sens de l'article 2, point 10), du règlement (CE) nº 765/2008;

7) «accréditation en portée flexible»: une accréditation dans laquelle les activités spécifiques d'évaluation de la conformité pour lesquelles l'accréditation est demandée, ou a été accordée, sont exprimées de manière à permettre aux organismes d'évaluation de la conformité d'apporter des modifications à leur méthodologie et à d'autres paramètres relevant de la compétence de l'organisme d'évaluation de la conformité, telle qu'elle a été confirmée par l'organisme national d'accréditation;

8) «organisme national d'accréditation»: un organisme national d'accréditation tel que défini à l'article 2, point 11), du règlement (CE) nº 765/2008.

([7]) 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) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([8]) EDPS Formal comments on the draft regarding the accreditation of conformity assessment bodies performing the assessment of qualified trust service providers and the qualified trust services they provide | Contrôleur européen de la protection des données.

Article 2

Accréditation des organismes d'évaluation de la conformité

1. Pour pouvoir prendre des décisions de certification conformément à un système d'évaluation de la conformité donné, les organismes d'évaluation de la conformité sont accrédités conformément à la norme EN ISO/IEC 17065:2012 complétée par la norme ETSI EN 319 403-1 v2.3.1.

2. L'accréditation des organismes d'évaluation de la conformité visés au paragraphe 1 est effectuée par un organisme national d'accréditation conformément à la norme EN ISO/IEC 17011:2017.

Article 3

Certificat d'accréditation délivré aux organismes d'évaluation de la conformité

1. Les organismes nationaux d'accréditation veillent à ce que les certificats d'accréditation qu'ils délivrent aux organismes d'évaluation de la conformité contiennent au moins les informations suivantes:

a) le code d'identification unique du certificat d'accréditation;

b) la date de délivrance du certificat d'accréditation;

c) le nom et le pays, tels qu'ils figurent dans les registres officiels nationaux, de l'organisme national d'accréditation délivrant le certificat d'accréditation;

d) le nom et, le cas échéant, le numéro d'immatriculation de l'organisme d'évaluation de la conformité accrédité, tels qu'ils figurent dans les registres officiels nationaux;

e) la portée de l'accréditation, en ce qui concerne un ou plusieurs des services de confiance qualifiés suivants:

— la délivrance de certificats qualifiés de signature électronique,

— la délivrance de certificats qualifiés de cachet électronique,

— la délivrance de certificats qualifiés d'authentification de site internet,

— le service de validation qualifié des signatures électroniques qualifiées,

— le service de validation qualifié des cachets électroniques qualifiés,

— le service qualifié de préservation des signatures électroniques qualifiées,

— le service qualifié de préservation des cachets électroniques qualifiés,

— la création d'horodatages électroniques qualifiés,

— la fourniture de services d'envoi recommandé électronique,

— le service qualifié de gestion de dispositifs de création de signature électronique qualifiés à distance,

— le service qualifié de gestion de dispositifs de création de cachet électronique qualifiés à distance,

— la fourniture de services d'archivage électronique qualifiés,

— la délivrance d'attestations électroniques d'attributs qualifiées,

— l'enregistrement de données électroniques dans un registre électronique qualifié;

f) l'identification, y compris, le cas échéant, la version spécifique, du système d'évaluation de la conformité pour lequel l'organisme d'évaluation de la conformité a été accrédité;

g) une mention indiquant que l'accréditation en portée flexible est utilisée, le cas échéant;

h) le cas échéant, la mention du document décrivant le processus de conception et de mise en œuvre de l'accréditation en portée flexible.

2. Les organismes nationaux d'accréditation veillent à ce que la date de début et, le cas échéant, la date de fin de l'accréditation de l'organisme d'évaluation de la conformité pour la réalisation de l'évaluation de la conformité des services de confiance qualifiés visés au paragraphe 1, point e), y compris les dates spécifiques pour chaque service de confiance qualifié, le cas échéant, fassent partie des informations d'accréditation mentionnées à l'article 20, paragraphe 1 *ter*, du règlement (UE) nº 910/2014.

3. Les organismes nationaux d'accréditation veillent à ce que toute modification pertinente apportée aux informations fournies conformément au paragraphe 1 apparaisse clairement dans le certificat d'accréditation.

4. Le certificat d'accréditation décrit clairement la portée de l'accréditation de l'organisme d'évaluation de la conformité, conformément à l'article 2, paragraphe 1.

Article 4

Réexamen de l'accréditation existante

1. Le propriétaire du système met en œuvre des procédures pour surveiller toute éventuelle modification apportée aux normes visées à l'article 2, paragraphe 1, ou à l'article 6, paragraphe 3, ou à un système d'évaluation de la conformité dont il est propriétaire et sur la base duquel un organisme d'évaluation de la conformité a été accrédité conformément à l'article 2.

2. Le propriétaire du système notifie en temps utile à l'organisme national d'accréditation les modifications constatées à l'issue des procédures prévues au paragraphe 1.

3. Lorsque l'organisme national d'accréditation n'a pas appliqué d'accréditation en portée flexible aux organismes d'évaluation de la conformité accrédités, il détermine si les modifications constatées à l'issue des procédures prévues au paragraphe 1 sont susceptibles d'affecter sensiblement la capacité des organismes d'évaluation de la conformité accrédités à effectuer des évaluations de la conformité conformément aux systèmes pour lesquels ils ont été accrédités.

4. Lorsque l'organisme national d'accréditation constate, conformément au paragraphe 3, que des modifications affectent la capacité des organismes d'évaluation de la conformité à effectuer des évaluations de la conformité, il demande à l'organisme d'évaluation de la conformité de prendre les mesures appropriées dans un délai raisonnable prescrit.

5. Si l'organisme d'évaluation de la conformité ne peut ou ne souhaite pas prendre les mesures visées au paragraphe 4 dans le délai prescrit, l'organisme national d'accréditation retire ou suspend immédiatement l'accréditation.

6. Lorsque l'organisme national d'accréditation détermine, conformément au paragraphe 3, que les modifications n'affectent pas la capacité des organismes d'évaluation de la conformité à effectuer des évaluations de la conformité, il peut, le cas échéant, étendre la validité et la portée de l'accréditation de l'organisme d'évaluation de la conformité évalué.

7. Le cas échéant, l'organisme national d'accréditation met à jour le certificat d'accréditation en temps voulu afin de tenir compte des résultats du réexamen de l'accréditation conformément au présent article.

8. Lorsqu'un organisme d'évaluation de la conformité reçoit une demande en vertu du paragraphe 4, il informe en temps utile tout prestataire de services de confiance qualifié qu'il a précédemment évalué dans le cadre du système d'évaluation de la conformité pertinent de toute incidence que le réexamen de l'accréditation de l'organisme d'évaluation de la conformité peut avoir sur ces prestataires de services de confiance qualifiés, y compris en ce qui concerne les futures décisions de certification prises par l'organisme d'évaluation de la conformité dans le cadre de ce système.

Article 5

Organismes d'évaluation de la conformité

1. Les organismes d'évaluation de la conformité mettent à disposition les certificats de conformité qu'ils délivrent dans un répertoire public qu'ils tiennent à jour à cet effet.

2. Toute sous-traitance, par l'organisme d'évaluation de la conformité, de l'exécution des activités d'évaluation de la conformité tient dûment compte de la nature de l'activité à réaliser. L'organisme d'évaluation de la conformité s'assure que le sous-traitant respecte les normes énoncées à l'annexe I pour l'activité spécifique sous-traitée.

3. Lorsqu'ils adoptent une décision de certification, les organismes d'évaluation de la conformité veillent à ce que le prestataire de services de confiance qualifié auquel la décision se rapporte soit en mesure de soumettre aux organes de contrôle les rapports complets d'évaluation de la conformité correspondant à cette décision.

Article 6

Systèmes d'évaluation de la conformité

1. Chaque système d'évaluation de la conformité fournit des données d'identification du propriétaire du système.

2. Un système d'évaluation de la conformité est conforme au programme de type 6 de la norme EN ISO/IEC 17067:2013 et aux exigences énoncées dans le présent article.

3. Les propriétaires de systèmes veillent à ce que leurs systèmes d'évaluation de la conformité comprennent au moins les normes énoncées à l'annexe II, selon le cas, en indiquant l'année et le numéro de version de ces normes.

4. Les propriétaires de systèmes font en sorte que l'éventuelle application d'une accréditation en portée flexible soit indiquée dans le système d'évaluation de la conformité.

5. Les propriétaires de systèmes veillent à ce que leurs programmes d'évaluation de la conformité établissent des processus et des procédures concernant au moins les éléments suivants:

a) la réception et le traitement des plaintes adressées au propriétaire du système concernant la mise en œuvre du système d'évaluation de la conformité;

b) les notifications adressées par l'organisme d'évaluation de la conformité à l'organe de contrôle désigné conformément à l'article 46 *ter*, paragraphe 1, du règlement (UE) nº 910/2014 concernant la délivrance des certificats de conformité et toute modification apportée à ceux-ci;

c) le cas échéant, la sous-traitance de l'exécution des activités d'évaluation de la conformité par l'organisme d'évaluation de la conformité;

d) la réalisation d'activités de surveillance annuelles sur la base des exigences applicables du paragraphe 7.9 de la norme ISO/IEC 17065:2012;

e) la gestion et la notification par le prestataire de services de confiance qualifié à l'organisme d'évaluation de la conformité et à l'organe de contrôle compétent de toute modification ayant une incidence sur le fonctionnement des prestataires de services de confiance qualifiés ou des services de confiance qualifiés qu'ils fournissent;

f) la vérification des éléments de preuve démontrant que l'organisme d'évaluation de la conformité:

— possède des connaissances et une expertise suffisantes en ce qui concerne l'application des normes spécifiques relatives au service de confiance qualifié fourni par le prestataire de services de confiance qualifié, tel que visé au paragraphe 3,

— possède une expérience professionnelle de l'évaluation de la conformité dans au moins trois évaluations de prestataires de services de confiance ou trois évaluations de systèmes de gestion de la sécurité de l'information, et

— peut garantir la disponibilité d'une équipe d'au moins deux personnes qualifiées possédant l'expertise nécessaire pour procéder à cette évaluation de la conformité.

6. Les propriétaires de systèmes veillent à ce que leurs systèmes d'évaluation de la conformité exigent des prestataires de services de confiance qualifiés qu'ils mettent en place des processus, des procédures et des instructions de travail pour faire en sorte que l'organisme d'évaluation de la conformité soit informé au moins un mois à l'avance lorsque les prestataires de services de confiance qualifiés mettent en œuvre une éventuelle modification importante dans la fourniture des services de confiance qualifiés certifiés dans le cadre de ce système et au moins trois mois à l'avance lorsqu'ils ont l'intention de mettre un terme à la fourniture de tout ou partie des services.

7. Les propriétaires de systèmes veillent à ce que leurs schémas d'évaluation de la conformité ne permettent pas la délivrance de décisions de certification positives ou de certificats de conformité lorsque l'évaluation de la conformité met en évidence une non-conformité des prestataires de services de confiance qualifiés évalués et du service de confiance qualifié qu'ils fournissent aux exigences du règlement (UE) nº 910/2014 et de l'article 21 de la directive (UE) 2022/2555.

8. Les propriétaires de systèmes veillent à ce que leurs systèmes d'évaluation de la conformité définissent la procédure relative à la délivrance d'un certificat de conformité. Ils exigent notamment que les prestataires de services de confiance qualifiés informent immédiatement l'organe de contrôle compétent de toute modification apportée à un certificat de conformité. Ils exigent également que les prestataires de services de confiance qualifiés s'abstiennent de fournir les services de confiance qualifiés concernés ou de publier d'éventuelles références à ces services jusqu'à ce que l'organe de contrôle compétent confirme à nouveau le statut qualifié. Cette procédure est conforme aux exigences énoncées au paragraphe 7.11 de la norme ISO/IEC 17065:2012.

9. Les propriétaires de systèmes veillent à ce que leurs programmes d'évaluation de la conformité définissent le processus d'évaluation de la conformité à exécuter sur un nombre suffisant de personnes-jours et veillent à ce que les ressources et le temps alloués à l'évaluation de la conformité soient suffisants compte tenu de la portée et de la complexité de l'évaluation.

10. Les propriétaires de systèmes publient un résumé du système d'évaluation de la conformité à des fins de téléchargement. Le résumé contient une description de l'ensemble des règles et procédures suivies pour évaluer la conformité des prestataires de services de confiance qualifiés et des services de confiance qualifiés qu'ils fournissent aux exigences du règlement (UE) n° 910/2014 et de l'article 21 de la directive (UE) 2022/2555.

11. Les propriétaires de systèmes veillent à ce que leurs programmes d'évaluation de la conformité exigent qu'au moins une évaluation de surveillance soit effectuée chaque année pour chaque service de confiance qualifié évalué.

Article 7

Rapports d'évaluation de la conformité

1. Le rapport d'évaluation de la conformité visé à l'article 20, paragraphe 1, du règlement (UE) n° 910/2014 est conforme aux spécifications énoncées à l'annexe III.

2. Le rapport d'évaluation de la conformité est considéré comme faisant partie de la documentation de certification figurant au paragraphe 7.7 de la norme ETSI EN 319 403-1.

Article 8

Informations relatives à l'accréditation

1. Toute partie intéressée peut demander gratuitement des informations actuelles et anciennes sur la portée, la date de début et, le cas échéant, la date de fin de l'accréditation des organismes d'évaluation de la conformité, pour chaque type de service de confiance qualifié que l'organisme d'évaluation de la conformité est ou a été accrédité pour évaluer. Ces informations sont mises à disposition par les organismes nationaux d'accréditation.

2. Les informations actuelles et anciennes visées au paragraphe 1 devraient être mises à disposition pendant une période d'au moins 6 ans après l'accréditation de l'organisme d'évaluation de la conformité.

Article 9

Clause de maintien des acquis

Les organismes d'évaluation de la conformité qui, avant le 17 novembre 2025, ont été accrédités conformément à la norme ETSI EN 319 403 version 2.2.2, ou à une version antérieure, aux fins de l'évaluation de la conformité au règlement (UE) n° 910/2014 des prestataires de services de confiance qualifiés et des services de confiance qualifiés qu'ils fournissent, sont réputés satisfaire aux exigences de l'article 2, paragraphe 1, jusqu'au 17 mai 2027.

Article 10

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 27 octobre 2025.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE I

Normes de référence pour la sous-traitance d'activités d'évaluation de la conformité

1) EN ISO/CEI 17025:2017 pour les activités d'essai.
2) EN ISO/IEC 17021-1: 2015 pour l'audit des systèmes de management.
3) EN ISO/IEC 17020:2012 pour les activités d'inspection.
4) EN ISO/IEC 17065:2012 pour les activités d'évaluation de la conformité.

ANNEXE II

Normes de référence pour les systèmes d'évaluation de la conformité

Les normes visées à l'article 6, paragraphe 3, sont ETSI TS 119 612 v2.4.1, ainsi que les normes suivantes:

Services de confiance qualifiés	Normes pertinentes
Délivrance de certificats qualifiés de signature électronique	— ETSI EN 319 411-2 — ETSI EN 301 549 — ETSI EN 319 412-1 — ETSI EN 319 412-2 — ETSI EN 319 412-5 — ETSI TS 119 461 — ETSI EN 319 401
Délivrance de certificats qualifiés de cachet électronique	— ETSI EN 319 411-2 — ETSI TS 119 495 — ETSI EN 301 549 — ETSI EN 319 412-1 — ETSI EN 319 412-2 — ETSI EN 319 412-3 — ETSI EN 319 412-5 — ETSI TS 119 461 — ETSI EN 319 401
Délivrance de certificats qualifiés d'authentification de site internet	— ETSI EN 319 411-2 — ETSI TS 119 411-5 — ETSI TS 119 495 — ETSI EN 301 549 — ETSI EN 319 412-1 — ETSI EN 319 412-4 — ETSI EN 319 412-5 — ETSI TS 119 461 — ETSI EN 319 401
Service de validation qualifié des signatures électroniques qualifiées	— ETSI TS 119 441 — ETSI TS 119 442 — ETSI EN 319 102-1 — ETSI TS 119 102-2 — ETSI TS 119 172-4 — ETSI EN 301 549 — ETSI EN 319 401
Service de validation qualifié des cachets électroniques qualifiés	— ETSI TS 119 441 — ETSI TS 119 442 — ETSI EN 319 102-1 — ETSI TS 119 102-2 — ETSI TS 119 172-4 — ETSI EN 301 549 — ETSI EN 310 401
Service qualifié de préservation des signatures électroniques qualifiées	— ETSI TS 119 511 — ETSI TS 119 172-4 — ETSI TS 119 512 — ETSI EN 301 549 — ETSI EN 310 401
Service qualifié de préservation des cachets électroniques qualifiés	— ETSI TS 119 511 — ETSI TS 119 172-4 — ETSI TS 119 512 — ETSI EN 301 549 — ETSI EN 319 401
Création d'horodatages électroniques qualifiés	— ETSI EN 319 421 — ETSI EN 319 422 — ETSI EN 301 549 — ETSI EN 319 401

Services de confiance qualifiés	Normes pertinentes
Fourniture de services d'envoi recommandé électronique	— ETSI EN 319 521 — ETSI EN 319 522 — ETSI EN 319 531 — ETSI EN 319 532 — ETSI EN 301 549 — ETSI TS 119 461 — ETSI EN 319 401
Service qualifié de gestion de dispositifs de création de signature électronique qualifiés à distance	— ETSI TS 119 431-1 — ETSI EN 301 549 — ETSI TS 119 461 — ETSI EN 319 401
Service qualifié de gestion de dispositifs de création de cachet électronique qualifiés à distance	— ETSI TS 119 431-1 — ETSI EN 301 549 — ETSI TS 119 461 — ETSI EN 319 401
Fourniture de services d'archivage électronique qualifiés	— ISO 14641 — ISO 14721 — CEN/TS 18170 — ETSI TS 301 549 — ETSI EN 319 401 — ETSI EN 119 511
Délivrance d'attestations électroniques d'attributs qualifiées	— ETSI TS 119 471 — ETSI EN 301 549 — ETSI TS 119 461 — ETSI EN 319 401
Enregistrement de données électroniques dans un registre électronique qualifié	— ETSI EN 319 401 — ETSI EN 301 549 — CEN/TS 18170 — ISO 23257 — ISO/TS 23635 — ETSI EN 319 122-1 — ETSI EN 319 132-1 — ETSI EN 319 182-1

ANNEXE III

Spécifications relatives aux rapports d'évaluation de la conformité

Le rapport d'évaluation de la conformité visé à l'article 7, paragraphe 1,

1) est accompagné d'une décision de certification claire conformément au paragraphe 7.6 de la norme ETSI EN 319403-1 v2.3.1 («ETSI EN 319403-1»), indiquant si le prestataire de services de confiance évalué et les services de confiance qualifiés évalués qu'il fournit ou vise à fournir satisfont aux exigences énoncées dans le règlement (UE) nº 910/2014 et à l'article 21 de la directive (UE) 2022/2555;

2) précise le nom du prestataire de services de confiance qualifié et, le cas échéant, son numéro d'immatriculation, tel qu'il figure dans les registres officiels, son adresse postale officielle et son adresse électronique, ainsi que, le cas échéant, les mêmes informations pour toutes les filiales, entités juridiques affiliées, contractants et sous-traitants qui exploitent des composantes de services de confiance relevant de la fourniture des services de confiance qualifiés par le prestataire de services de confiance qualifié;

3) comprend une description détaillée de la portée de l'évaluation du prestataire de services de confiance qualifié, y compris des services de confiance qualifiés spécifiques couverts par l'évaluation;

4) contient suffisamment d'éléments démontrant que le prestataire de services de confiance et les services de confiance qualifiés qu'il a l'intention de fournir respectent les exigences énoncées dans le règlement (UE) nº 910/2014 et à l'article 21 de la directive (UE) 2022/2555;

5) le nom de l'organisme d'évaluation de la conformité et, le cas échéant, son numéro d'immatriculation, tels qu'ils figurent dans les registres officiels, son adresse postale enregistrée et son adresse électronique;

6) précise les informations suivantes:

   a) le nom et le pays de l'organisme national d'accréditation ayant accrédité l'organisme d'évaluation de la conformité;

   b) le nom des personnes physiques que l'organisme d'évaluation de la conformité charge de participer à l'évaluation de la conformité et leur rôle respectif dans cette évaluation;

   c) le lien vers le site internet officiel de l'organisme national d'accréditation, contenant le certificat d'accréditation délivré par l'organisme national d'accréditation à l'organisme d'évaluation de la conformité;

   d) le cas échéant, le symbole d'accréditation numérique;

   e) le système d'évaluation de la conformité pour lequel l'organisme d'évaluation de la conformité a été accrédité conformément à l'article 2, paragraphe 1;

   f) les renseignements relatifs à l'évaluation de la conformité demandés dans le cadre de l'évaluation de la conformité effectuée, les motifs justifiant leur sélection et la méthodologie utilisée, y compris la méthode d'échantillonnage et les procédures d'essai;

   g) le système d'évaluation de la conformité accrédité et les documents pertinents ou un lien vers l'endroit où ce système d'évaluation de la conformité et les documents pertinents sont disponibles;

7) contient au moins une signature électronique qualifiée, si le rapport est fourni sous forme électronique, ou une signature manuscrite, s'il est fourni sur support papier, indiquant le nom et le titre de la ou des personnes responsables qui ont été habilitées à adopter la décision de certification au nom de l'organisme d'évaluation de la conformité;

8) concerne un prestataire de services de confiance qualifié;

9) énumère, conformément au paragraphe 5.5.3 de la norme ETSI TS 119612 v.2.4.1, les identités numériques du service par type de service de confiance qualifié pour lequel il confirme la conformité aux exigences énoncées dans le règlement (UE) nº 910/2014 et à l'article 21 de la directive (UE) 2022/2555, en fournissant les informations suivantes:

   a) lorsque le service de confiance qualifié n'est pas fondé sur une technologie d'infrastructure à clé publique, un identifiant exprimé sous la forme d'un URI qui identifie de manière unique le service de confiance qualifié;

   b) lorsque le service de confiance qualifié est fondé sur une technologie d'infrastructure à clé publique, au moins les éléments suivants:

      — l'identifiant de clé de l'objet (*Subject Key identifier*) tel que défini dans le RFC 5280 de l'IETF;

      — la représentation en Base64 PEM du certificat numérique X.509v3 associé;

— le cas échéant, une mention indiquant si des ensembles ou sous-ensembles spécifiques de certificats d'entité finale délivrés par l'identité numérique du service ou dans le cadre de celle-ci sont exclus de la décision de certification ou expressément inclus dans cette décision et sur la base de quels critères ils peuvent être identifiés;

— une mention indiquant si l'identité numérique du service concerne une entité finale ou une autorité de certification, précisant s'il s'agit d'un certificat émis, intermédiaire ou racine;

— une description de la manière dont l'identité numérique du service est utilisée dans le cadre du service de confiance qualifié correspondant;

10) fournit, le cas échéant, une description détaillée de la hiérarchie fonctionnelle de l'infrastructure à clé publique, par type de service de confiance qualifié et pour toutes les identités numériques du service identifiées conformément au point 11, comprenant au moins:

a) l'illustration de la hiérarchie des infrastructures à clé publique identifiant les autorités de certification racine, les autorités de certification intermédiaires, les autorités de certification émettrices et les chemins de certification qui les relient;

b) l'identification de chaque autorité de certification illustrée au point a) au moyen de l'identifiant de la clé du sujet tel que défini dans le RFC 5280 de l'IETF;

c) pour chacune des autorités de certification émettrices identifiées conformément au point b), la liste des différents ensembles de certificats que chaque autorité de certification délivre en fonction de ses politiques de certification, ainsi que, pour chacun de ces ensembles:

— des critères qui identifient sans ambiguïté les certificats de l'ensemble, qui sont soit une liste d'identifiants de la politique de certification correspondant au contenu de l'extension concernant la politique de certification, telle que définie dans le RFC 5280 de l'IETF, soit d'autres critères définis dans les actes d'exécution adoptés en vertu de l'article 22, paragraphe 5, du règlement (UE) nº 910/2014,

— une mention indiquant si les certificats de l'ensemble sont qualifiés ou non,

— une mention indiquant si les certificats de l'ensemble sont destinés à des signatures électroniques, à des cachets électroniques, à une authentification de site internet ou à aucune de ces fins et, dans ce dernier cas, à quelles autres fins leur utilisation est prévue,

— une mention indiquant si la clé privée correspondant à la clé publique certifiée dans les certificats des ensembles réside dans un dispositif de création de signature qualifiée ou de cachet qualifié local ou à distance;

11) comprend, conformément au point 2

a) une liste exhaustive des tiers, y compris de sous-traitants, qui fournissent des composants de services de confiance qualifiés ou des composants de services, indiquant leur nom, tel que prévu au point 2, ainsi que l'emplacement des sites où les composants de services correspondants sont exploités;

b) une mention indiquant si ces tiers et sites ont fait l'objet de l'évaluation de la conformité et dans quelle mesure;

12) décrit, le cas échéant, le contenu de l'inscription à ajouter ou à mettre à jour dans la liste de confiance nationale pertinente, en fonction du résultat de l'évaluation;

13) inclut une liste exhaustive des documents internes des prestataires de services de confiance publics et qualifiés, dûment identifiés, y compris les versions, qui ont été couverts par la portée de l'évaluation de la conformité, y compris au moins les documents suivants visés au point 8, pour lesquels une copie est soit fournie en même temps que le rapport d'évaluation de la conformité, soit mise à la disposition de l'organe de contrôle compétent à sa demande:

a) la déclaration des pratiques utilisées par le prestataire de services de confiance qualifié pour fournir les services de confiance qualifiés;

b) l'ensemble de règles indiquant l'applicabilité des services de confiance qualifiés à une communauté ou à une catégorie d'application particulière ayant des exigences communes en matière de sécurité («politiques en matière de services de confiance qualifiés»);

c) les modalités et conditions relatives aux accords d'abonnés;

d) le plan d'arrêt des services de confiance qualifiés;

e) la documentation liée à l'évaluation des risques, qui vise à démontrer que les exigences de l'article 24, paragraphe 2, points f *bis*) et f *ter*), du règlement (UE) nº 910/2014 et de l'article 21 de la directive (UE) 2022/2555 ont été respectées;

f) le plan de notification des atteintes à la sécurité, qui vise à démontrer que les exigences de l'article 24, paragraphe 2, points f *bis*) et f *ter*), du règlement (UE) nº 910/2014 et de l'article 21 de la directive (UE) 2022/2555 ont été respectées;

g) la liste de tous les documents internes étayant la mise en œuvre effective des pratiques déclarées et utilisées par le prestataire de services de confiance qualifié pour fournir les services de confiance qualifiés;

h) l'acte constitutif et les statuts du prestataire de services de confiance qualifié, conformément au droit national applicable, ainsi que les éléments suivants:

— une déclaration d'activités commerciales non liées à la fourniture de services de confiance,

— un organigramme,

— des informations sur la structure de propriété,

— le cas échéant et s'il est disponible, le rapport du contrôleur des comptes de l'entreprise pour les deux exercices financiers précédents, ou de la date de la constitution de l'entreprise jusqu'à la date de signature du rapport d'évaluation de la conformité, la période la plus courte étant retenue;

i) la preuve que le prestataire de services de confiance qualifié, conformément au droit national applicable, dispose de ressources financières suffisantes et, le cas échéant, a obtenu une assurance de responsabilité civile appropriée en ce qui concerne la fourniture des services de confiance qualifiés;

j) la liste des normes auxquelles les opérations sont déclarées conformes;

k) la liste des normes au regard desquelles les opérations sont auditées, évaluées, certifiées ou jugées conformes, ainsi que des détails sur le système d'audit, d'évaluation, de certification ou d'évaluation de conformité sous-jacent, selon le cas;

l) la liste des dispositifs de création de signature électronique qualifiés ou des dispositifs de création de cachet électronique qualifiés et leurs informations relatives à la certification lorsque le prestataire de services de confiance qualifié fournit ces dispositifs à ses utilisateurs ou les met à leur disposition;

m) la liste des dispositifs que le prestataire de services de confiance qualifié utilise en tant que système ou produit fiable, y compris les modules de sécurité matériels ou les dispositifs cryptographiques sécurisés, pour protéger ses propres clés, et les informations relatives à leur certification, lorsque le prestataire de services de confiance qualifié utilise ces dispositifs pour sécuriser les processus soutenant les services de confiance qualifiés qu'il fournit;

14) contient une évaluation du respect des exigences qui s'appliquent aux services de confiance qualifiés concernés en vertu du règlement (UE) nº 910/2014 et, le cas échéant, telles qu'énoncées dans les actes d'exécution et les actes délégués qui s'appliquent à ce service de confiance qualifié, telles qu'adoptées conformément à:

— l'article 24, paragraphe 1 *quater*, du règlement (UE) nº 910/2014 en ce qui concerne la vérification de l'identité et des attributs des personnes auxquelles le certificat qualifié ou l'attestation électronique qualifiée doit être délivré,

— l'article 24, paragraphe 5, du règlement (UE) nº 910/2014 en ce qui concerne les exigences applicables aux prestataires de services de confiance qualifiés fournissant des services de confiance qualifiés,

— l'article 28, paragraphe 6, du règlement (UE) nº 910/2014 en ce qui concerne la délivrance de certificats qualifiés de signature électronique,

— l'article 38, paragraphe 6, du règlement (UE) nº 910/2014 en ce qui concerne la délivrance de certificats qualifiés de cachets électroniques,

— l'article 45, paragraphe 2, du règlement (UE) nº 910/2014 en ce qui concerne la délivrance de certificats qualifiés d'authentification de site internet,

— l'article 33, paragraphe 2, du règlement (UE) nº 910/2014 en ce qui concerne le service de validation qualifié des signatures électroniques qualifiées,

— l'article 33, paragraphe 2, et l'article 40 du règlement (UE) nº 910/2014 en ce qui concerne le service de validation qualifié des cachets électroniques qualifiés,

— l'article 34, paragraphe 2, du règlement (UE) nº 910/2014 en ce qui concerne le service qualifié de préservation des signatures électroniques qualifiées,

— l'article 34, paragraphe 2, et l'article 40 du règlement (UE) nº 910/2014 en ce qui concerne le service qualifié de préservation des cachets électroniques qualifiés,

— l'article 42, paragraphe 2, du règlement (UE) nº 910/2014 en ce qui concerne la création d'horodatages électroniques qualifiés,

— l'article 44, paragraphe 2, du règlement (UE) nº 910/2014 en ce qui concerne la fourniture de services d'envoi recommandé électronique qualifiés,

— l'article 29 *bis*, paragraphe 2, du règlement (UE) nº 910/2014 en ce qui concerne les services qualifiés de gestion de dispositifs de création de signature électronique qualifiés à distance,

— l'article 29 *bis*, paragraphe 2, et l'article 39 *bis* du règlement (UE) nº 910/2014 en ce qui concerne les services qualifiés de gestion de dispositifs de création de cachet électronique qualifiés à distance,

— l'article 45 *undecies*, paragraphe 2, du règlement (UE) nº 910/2014 en ce qui concerne la fourniture de services d'archivage électronique qualifiés,

— l'article 45 *quinquies*, paragraphe 5, du règlement (UE) nº 910/2014 en ce qui concerne la délivrance d'attestations électroniques qualifiées d'attributs,

— l'article 45 *terdecies*, paragraphe 3, du règlement (UE) nº 910/2014 en ce qui concerne l'enregistrement de données électroniques dans un registre électronique qualifié;

15) contient une évaluation du respect des exigences applicables au prestataire de services de confiance qualifié et aux services de confiance qualifiés pertinents en vertu de l'article 21 de la directive (UE) 2022/2555 et des actes d'exécution qui s'appliquent à ce service de confiance qualifié, tels qu'adoptés conformément à l'article 21, paragraphe 5, de ladite directive;

16) contient une déclaration établissant, le cas échéant, l'absence de toute non-conformité, quel que soit son niveau de criticité; lorsqu'une non-conformité est constatée dans le rapport, celui-ci fournit un plan de mesures correctives et leur calendrier, communiqué par le prestataire de services de confiance qualifié et approuvé par l'organisme d'évaluation de la conformité, accompagné de la description des tâches d'évaluation que l'organisme d'évaluation de la conformité doit effectuer pour établir que ces non-conformités ont été corrigées;

17) contient, lorsque cela est approprié et nécessaire, une indication des possibilités d'amélioration en ce qui concerne le respect des exigences pertinentes par le prestataire de services de confiance qualifié et les services de confiance qualifiés qu'il fournit;

18) détermine, pour chaque étape de l'évaluation de la conformité, y compris l'audit documentaire, l'évaluation de la mise en œuvre et les inspections sur place, la période au cours de laquelle l'évaluation a été réalisée et le temps pris par l'organisme d'évaluation de la conformité, exprimé en personnes-jours, pour procéder à l'évaluation;

19) indique, dans chaque rapport relatif à une exigence spécifique, les contrôles et objectifs détaillés de l'évaluation de la conformité qui ont été effectués au cours de l'évaluation ou inclut une référence aux rapports d'évaluation disponibles séparément dans lesquels figurent ces informations, pour autant que ces rapports d'évaluation distincts soient:

a) délivrés par des organismes d'évaluation de la conformité accrédités conformément au règlement (UE) nº 910/2014;

b) avalisés par les organismes d'évaluation de la conformité délivrant le rapport d'évaluation de la conformité;

20) comprend la portée, la description et les résultats d'un ensemble significatif d'essais ou d'échantillons de production ainsi que leur évaluation pour tous les types pertinents et applicables de produits des services de confiance qualifiés évalués;

21) indique les délais suivants:

a) le délai dans lequel la prochaine évaluation de la conformité de surveillance doit être effectuée;

b) le délai dans lequel la prochaine évaluation de la conformité doit être effectuée conformément à l'article 20, paragraphe 1, du règlement (UE) n° 910/2014;

22) contient une déclaration indiquant explicitement que les documents de certification, y compris le rapport d'évaluation de la conformité, sont également destinés à être utilisés par l'organe national de contrôle compétent.

Journal officiel
de l'Union européenne

FR
Série L

2025/2530

17.12.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/2530 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 exigences applicables aux prestataires de services de confiance qualifiés fournissant des services de confiance 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 24, paragraphe 5,

considérant ce qui suit:

(1) Les prestataires de services de confiance qualifiés jouent un rôle essentiel pour assurer des interactions numériques sûres et fiables en fournissant des services de confiance qualifiés conformément au règlement (UE) nº 910/2014.

(2) La présomption de conformité prévue à l'article 24, paragraphe 5, du règlement (UE) nº 910/2014 ne devrait s'appliquer que lorsque les services de confiance qualifiés respectent les exigences et les normes de référence et spécifications énoncées dans le présent règlement. Ces exigences et ces normes de référence et spécifications devraient tenir compte des pratiques établies et être largement reconnues dans les secteurs concernés. Les normes de référence 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 et des prestataires de services de confiance qualifiés qui fournissent ce service.

(3) Si un prestataire de services de confiance respecte les exigences et les normes de référence et spécifications énoncées dans le 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, les pratiques et les normes ou spécifications techniques et de suivre les meilleures pratiques sur le marché intérieur.

(5) Il incombe aux prestataires de services de confiance qualifiés d'adresser une notification aux organes de contrôle avant d'apporter quelque modification que ce soit à la fourniture de leurs services de confiance qualifiés. Ces notifications devraient permettre aux organes de contrôle d'exiger des prestataires de services de confiance qualifiés qu'ils prennent des mesures appropriées pour atténuer les éventuelles incidences négatives des modifications notifiées quant au respect des exigences du règlement (UE) nº 910/2014 et à l'octroi du statut qualifié. Afin de fournir des précisions et des orientations aux prestataires de services de confiance qualifiés sur les modifications qu'il leur incombe de notifier aux organes de contrôle, le présent règlement devrait comprendre une liste non exhaustive de ces modifications.

([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) Nonobstant l'article 21 de la directive (UE) 2022/2555 du Parlement européen et du Conseil ([3]), l'article 24, paragraphe 2, du règlement (UE) n° 910/2014 prévoit des exigences supplémentaires en ce qui concerne les procédures de gestion des risques en matière de risques juridiques, commerciaux et opérationnels et autres risques directs ou indirects liés à la fourniture du service de confiance qualifié, qui ne relèvent pas du règlement d'exécution (UE) 2024/2690 de la Commission ([4]). Afin de garantir qu'ils évaluent et documentent structurellement et systématiquement ces risques liés à la fiabilité de leurs services de confiance qualifiés, les prestataires de services de confiance qualifiés devraient mettre en œuvre un cadre de gestion des risques adapté aux services de confiance qualifiés qu'ils fournissent. Afin de garantir la cohérence des procédures de gestion des risques mises en œuvre par les prestataires de services de confiance non qualifiés et les prestataires de services de confiance qualifiés, ce cadre devrait être conforme aux exigences énoncées dans le règlement d'exécution (UE) 2025/2160 de la Commission ([5]).

(7) La continuité des services de confiance qualifiés ou l'arrêt dans de bonnes conditions des services de confiance qualifiés lorsque leur continuité ne peut être assurée est un élément essentiel pour renforcer la fiabilité des services de confiance qualifiés. Des plans d'arrêt d'activité suffisamment détaillés constituent un outil important pour garantir que les abonnés et les parties utilisatrices peuvent se fier aux produits des services de confiance qualifiés en cas d'arrêt de ces services. Les plans d'arrêt d'activité devraient couvrir à la fois l'arrêt prévu d'un service de confiance qualifié, comme la vente d'un service de confiance qualifié à un autre prestataire de services de confiance qualifié, et l'arrêt imprévu, comme la faillite ou d'autres cas d'insolvabilité. Les plans d'arrêt d'activité devraient contenir des dispositions appropriées pour garantir que les effets de l'arrêt peuvent être gérés sans incidence négative sur la validité ou la valeur des produits générés par le service de confiance qualifié avant l'arrêt de son activité. En outre, les plans d'arrêt d'activité devraient garantir l'impossibilité d'obtenir de nouveaux produits d'un service de confiance qualifié dont l'activité a été arrêtée lorsqu'il ne satisfait plus aux exigences applicables aux services de confiance qualifiés ou aux prestataires de services de confiance qualifiés énoncées dans le règlement (UE) n° 910/2014. Les prestataires de services de confiance qualifiés devraient tenir à jour les plans d'arrêt d'activité et analyser l'incidence de toute modification apportée au prestataire de services de confiance qualifié ou aux services de confiance qualifiés qu'il fournit, telle qu'un changement de nom, une fusion, une acquisition, une faillite, un redressement judiciaire, une mise sous tutelle ou une modification technique, sur les plans d'arrêt d'activité avant de mettre en œuvre cette modification.

(8) La Commission a adopté des règlements d'exécution comprenant des références aux normes et spécifications techniques applicables aux services de confiance qualifiés. Ces règlements d'exécution, visés à l'annexe du présent règlement, précisent les modalités d'application et d'interprétation des exigences applicables aux prestataires de services de confiance qualifiés énoncées à l'article 24, paragraphe 2, du règlement (UE) n° 910/2014 compte tenu des spécificités de ces services de confiance qualifiés. Pour que la présomption de conformité énoncée à l'article 24, paragraphe 5, du règlement (UE) n° 910/2014 s'applique au prestataire de services qualifié, toutes les exigences mentionnées à l'annexe devraient être mises en œuvre telles qu'elles s'appliquent au service de confiance qualifié concerné.

(9) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([6]) et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([7]) s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du présent règlement.

([3]) Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([4]) Règlement d'exécution (UE) 2024/2690 de la Commission du 17 octobre 2024 établissant des règles relatives à l'application de la directive (UE) 2022/2555 pour ce qui est des exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité et précisant plus en détail les cas dans lesquels un incident est considéré comme important, en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance (JO L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

([5]) Règlement d'exécution (UE) 2025/2160 de la Commission du 27 octobre 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les normes de référence, les spécifications et les procédures applicables à la gestion des risques liés à la fourniture des services de confiance non qualifiés (JO L, 2025/2160, 28.10.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/2160/oj).

([6]) 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).

([7]) 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).

(10) 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 ([8]) et a rendu son avis le 21 octobre 2025 ([9]).

(11) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Notifications à l'organe de contrôle

1. Dans les notifications visées à l'article 24, paragraphe 2, point a), du règlement (UE) nº 910/2014, les prestataires de services de confiance qualifiés incluent au moins les modifications importantes apportées à l'ensemble des éléments suivants:

a) les descriptions de services, les politiques, les énoncés des pratiques ou les conditions et modalités associées;

b) l'architecture technique des services de confiance qualifiés ou les systèmes ou produits fiables visés à l'article 24, paragraphe 2, points e) et f), du règlement (UE) nº 910/2014;

c) l'hébergement des composants techniques nécessaires à la fourniture des services de confiance qualifiés ou les services techniques se rapportant à ces composants techniques;

d) l'utilisation de techniques ou matériels cryptographiques pour la fourniture des services de confiance qualifiés;

e) les procédures d'enregistrement et d'identification;

f) la structure organisationnelle ou la gouvernance du prestataire de services de confiance;

g) le plan d'arrêt d'activité;

h) les ressources financières et l'assurance responsabilité visées à l'article 24, paragraphe 2, point c), du règlement (UE) nº 910/2014;

i) les éléments ayant une incidence sur le contenu de la liste nationale de confiance correspondante;

j) les tiers intervenant dans la fourniture des services de confiance qualifiés, y compris les sous-traitants ou prestataires de services, ou les conditions contractuelles établies avec ces tiers.

2. Les notifications visées au paragraphe 1 comprennent:

a) la description de la modification;

b) la date et l'heure prévues de la modification;

c) les raisons de la modification et, le cas échéant, les éléments inhérents à ces raisons;

d) le cas échéant, les documents actualisés.

([8]) 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) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([9]) EDPS Formal comments on the draft Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards requirements for qualified trust service providers providing qualified trust services.

Article 2

Cadre de gestion des risques

Les exigences énoncées aux articles 2, 3 et 4 du règlement d'exécution (UE) 2025/2160 s'appliquent par analogie aux prestataires de services de confiance qualifiés en ce qui concerne l'exigence de prévoir un cadre de gestion des risques fixée à l'article 24, paragraphe 2, point f *bis*), du règlement (UE) nº 910/2014.

Article 3

Plan d'arrêt d'activité

1. Les prestataires de services de confiance qualifiés établissent un plan d'arrêt d'activité pour chaque service de confiance qualifié qu'ils fournissent, établissant les dispositions nécessaires à l'application efficace et correcte de l'arrêt de tout ou partie du service, aux fins d'assurer la continuité du service et de pouvoir fournir des preuves en justice, y compris les modalités selon lesquelles les informations sont maintenues accessibles conformément à l'article 24, paragraphe 2, point h), du règlement (UE) nº 910/2014.

2. Les prestataires de services de confiance qualifiés mettent en place des contrôles et des procédures visant à garantir la disponibilité, à des fins d'utilisation interne, de politiques, pratiques, procédures et accords avec des tiers documentés, ainsi que de tout autre document nécessaire pour assurer l'efficacité du plan d'arrêt d'activité.

3. Les prestataires de services de confiance qualifiés mettent en place des contrôles et des procédures visant à garantir que leur plan d'arrêt d'activité et tout document associé sont à jour.

4. Les prestataires de services de confiance qualifiés réexaminent le plan d'arrêt d'activité et tout document associé au moins tous les deux ans ainsi que lors de la mise en œuvre de toute modification apportée au prestataire de services de confiance qualifié ou aux services de confiance qualifiés qu'il fournit et mettent à jour le plan d'arrêt d'activité en conséquence.

5. Les prestataires de services de confiance qualifiés gèrent les risques propres à l'arrêt de la fourniture de leurs services de confiance qualifiés conformément au cadre de gestion des risques visé à l'article 2.

6. Les prestataires de services de confiance qualifiés garantissent le maintien de ressources financières suffisantes ou obtiennent des assurances suffisantes pour couvrir les coûts nécessaires à l'exécution efficace du plan d'arrêt d'activité, y compris en cas d'arrêt d'activité imprévu.

7. Les prestataires de services de confiance qualifiés veillent à ce que le plan d'arrêt d'activité précise les procédures et modalités appropriées sur les points suivants au minimum:

a) l'arrêt des services de confiance qualifiés, y compris, le cas échéant, en ce qui concerne le déclassement de tout composant technique ou service utilisé pour fournir le service de confiance qualifié concerné;

b) une mise à jour en temps utile des services connexes inscrits sur la liste nationale de confiance correspondante;

c) la révocation de tout certificat qualifié existant et non révoqué qu'ils ont délivré avant de conclure l'arrêt du service de confiance qualifié pour la délivrance de certificats qualifiés, sauf si toutes les obligations pertinentes des services de confiance qualifiés dont l'activité a été arrêtée sont transférées à un autre prestataire de services de confiance qualifié d'une manière garantissant que les certificats qualifiés et tous les services connexes continuent de satisfaire aux exigences du règlement (UE) nº 910/2014 de manière ininterrompue;

d) la garantie qu'après l'arrêt de la fourniture des services de confiance qualifiés, aucun nouveau produit de services de confiance qualifiés ne pourra être créé ou rendu possible en utilisant les données de création de signature ou de cachet du prestataire de services de confiance qualifié;

e) la garantie de l'accessibilité et de la facilité d'utilisation de tous les enregistrements pertinents détenus par le prestataire de services de confiance qualifié;

f) la prise en charge des scénarios d'arrêt d'activité prévu, imprévu, partiel et complet;

g) la garantie que les intérêts des abonnés des services de confiance qualifiés dont l'activité a été arrêtée soient préservés lors de l'arrêt d'activité, parmi lesquels la maintenance ininterrompue des informations nécessaires aux abonnés pour vérifier la validité juridique des produits des services de confiance qualifiés;

h) le cas échéant, l'indication des dispositions prises pour permettre la fourniture de services de confiance qualifiés alternatifs par d'autres prestataires de services de confiance qualifiés afin de réduire au minimum les perturbations pour les abonnés;

i) les notifications adressées aux parties connues du prestataire de services de confiance qualifié qui seront directement ou indirectement touchées par l'arrêt d'activité.

8. Les procédures et modalités visées au paragraphe 7, point e), garantissent l'accessibilité et la facilité d'utilisation des enregistrements nécessaires pour:

a) apporter la preuve de la conformité des services de confiance qualifiés avec le règlement (UE) n° 910/2014 et le règlement (UE) 2016/679;

b) assurer la continuité des services de confiance qualifiés, en ce qui concerne les données de validation de signature ou de cachet du prestataire de services de confiance qualifié et en ce qui concerne les conditions de maintenance ininterrompue des informations nécessaires pour vérifier l'exactitude des produits de services de confiance créés antérieurement.

9. Les prestataires de services de confiance qualifiés veillent à ce que le plan d'arrêt d'activité et les enregistrements associés contiennent au moins les documents suivants:

a) les procédures d'arrêt d'activité des services de confiance qualifiés;

b) les procédures et les enregistrements relatifs au réexamen régulier du plan d'arrêt d'activité visé au paragraphe 4;

c) les rapports d'audit relatifs au plan d'arrêt d'activité;

d) les modalités d'arrêt d'activité établies avec les tiers intervenant dans la fourniture des services de confiance qualifiés dont il est prévu d'arrêter l'activité;

e) les conditions et modalités, pratiques et documents sur les politiques se rapportant aux services de confiance qualifiés.

Article 4

Normes de référence et spécifications pour les services de confiance qualifiés

1. Outre les exigences énoncées aux articles 1er, 2 et 3, les normes de référence et spécifications visées à l'article 24, paragraphe 5, du règlement (UE) n° 910/2014 figurent à l'annexe du présent règlement.

2. En cas de divergences entre les normes de référence et spécifications établies par les règlements d'exécution et figurant à l'annexe du présent règlement et les exigences énoncées aux articles 1er, 2 et 3 du présent règlement, les exigences énoncées aux articles 1er, 2 et 3 du présent règlement prévalent.

Article 5

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

ANNEXE

Liste des normes de référence et des spécifications mentionnées à l'article 4

1) En ce qui concerne les services de confiance qualifiés pour la délivrance de certificats qualifiés de signature électronique: paragraphes 5.2, 6.1, 6.4, 6.5, 6.8 et 6.9 de la norme, tels que mentionnés et adaptés au point 1 de l'annexe I du règlement d'exécution (UE) 2025/1943 de la Commission ([1]).

2) En ce qui concerne les services de confiance qualifiés pour la délivrance de certificats qualifiés de cachet électronique: paragraphes 5.2, 6.1, 6.4, 6.5, 6.8 et 6.9 de la norme, tels que mentionnés et adaptés au point 1 de l'annexe II du règlement d'exécution (UE) 2025/1943.

3) En ce qui concerne les services de confiance qualifiés pour la délivrance de certificats qualifiés d'authentification de site internet: paragraphes 5.2, 6.1, 6.4, 6.5, 6.8 et 6.9 de la norme, tels que mentionnés et adaptés à l'annexe du règlement d'exécution (UE) 2025/1943.

4) En ce qui concerne les services de validation qualifiés des signatures électroniques qualifiées: paragraphes 5, 6 et 7 de la norme, tels que mentionnés et adaptés au point 1 de l'annexe du règlement d'exécution (UE) 2025/1942 de la Commission ([2]).

5) En ce qui concerne les services de validation qualifiés des cachets électroniques qualifiés: paragraphes 5, 6 et 7 de la norme, tels que mentionnés et adaptés au point 1 de l'annexe du règlement d'exécution (UE) 2025/1942.

6) En ce qui concerne les services qualifiés de préservation des signatures électroniques qualifiées: paragraphes 5, 6 et 7 de la norme, tels que mentionnés et adaptés au point 1 de l'annexe du règlement d'exécution (UE) 2025/1946 de la Commission ([3]).

7) En ce qui concerne les services qualifiés de préservation des cachets électroniques qualifiées: paragraphes 5, 6 et 7 de la norme, tels que mentionnés et adaptés au point 1 de l'annexe du règlement d'exécution (UE) 2025/1946.

8) En ce qui concerne les services de confiance qualifiés pour la création d'horodatages électroniques qualifiés: paragraphes 5, 6 et 7 de la norme, tels que mentionnés et adaptés au point 1 de l'annexe du règlement d'exécution (UE) 2025/1929 de la Commission ([4]).

9) En ce qui concerne les services d'envoi recommandé électronique qualifiés: paragraphes 4, 6 et 7 de la norme, tels que mentionnés et adaptés à l'annexe I du règlement d'exécution (UE) 2025/1944 de la Commission ([5]).

([1]) Règlement d'exécution (UE) 2025/1943 de la Commission du 29 septembre 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les normes de référence applicables aux certificats qualifiés de signature électronique et aux certificats qualifiés de cachet électronique (JO L, 2025/1943, 30.9.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1943/oj).

([2]) Règlement d'exécution (UE) 2025/1942 de la Commission du 29 septembre 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les services de validation qualifiés des signatures électroniques qualifiées et les services de validation qualifiés des cachets électroniques qualifiés (JO L, 2025/1942, 30.9.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1942/oj).

([3]) Règlement d'exécution (UE) 2025/1946 de la Commission du 29 septembre 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les services qualifiés de préservation des signatures électroniques qualifiées et des cachets électroniques qualifiés (JO L, 2025/1946, 30.9.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1946/oj).

([4]) Règlement d'exécution (UE) 2025/1929 de la Commission du 29 septembre 2025 portant modalités d'application du règlement (UE) n° 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 (JO L, 2025/1929, 30.9.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1929/oj).

([5]) Règlement d'exécution (UE) 2025/1944 de la Commission du 29 septembre 2025 portant modalités d'application du règlement (UE) n° 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 (JO L, 2025/1944, 30.9.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1944/oj).

10) En ce qui concerne les services qualifiés de gestion de dispositifs de création de signature électronique qualifiés à distance: paragraphes 5, 6.1, 6.4, 6.5, 6.7 et 6.8 de la norme, tels que mentionnés et adaptés à l'annexe du règlement d'exécution (UE) 2025/1567 de la Commission ([6]).

11) En ce qui concerne les services qualifiés de gestion de dispositifs de création de cachet électronique qualifiés à distance: paragraphes 5, 6.1, 6.4, 6.5, 6.7 et 6.8 de la norme, tels que mentionnés et adaptés à l'annexe du règlement d'exécution (UE) 2025/1567.

12) En ce qui concerne les services d'archivage électronique qualifiés: paragraphes 6 et 7 de la norme, tels que mentionnés et adaptés à l'annexe du règlement d'exécution (UE) 2025/2532 de la Commission ([7]).

13) En ce qui concerne les services de confiance qualifiés pour la délivrance d'attestations électroniques d'attributs qualifiées: la norme mentionnée à l'annexe I du règlement d'exécution (UE) 2025/1569 de la Commission ([8]).

14) En ce qui concerne les services de confiance qualifiés pour l'enregistrement de données électroniques dans un registre électronique qualifié: la norme mentionnée et adaptée au point 3, a), de l'annexe du règlement d'exécution (UE) 2025/2531 de la Commission ([9]).

([6]) Règlement d'exécution (UE) 2025/1567 de la Commission du 29 juillet 2025 portant modalités d'application du règlement (UE) n° 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 (OJ L, 2025/1567, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1567/oj).

([7]) Règlement d'exécution (UE) 2025/2532 de la Commission du 16 décembre 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les normes de référence et les spécifications applicables aux services d'archivage électronique qualifiés (JO L, 2025/2532, 17.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/2532/oj).

([8]) Règlement d'exécution (UE) 2025/1569 de la Commission du 29 juillet 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les attestations électroniques d'attributs qualifiées et les attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte (JO L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([9]) Règlement d'exécution (UE) 2025/2531 de la Commission du 16 décembre 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les normes de référence et les spécifications applicables aux registres électroniques qualifiés (JO L, 2025/2531, 17.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/2531/oj).

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).

Journal officiel
de l'Union européenne

FR
Série L

2025/2532

17.12.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/2532 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 services d'archivage électronique 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 *undecies*, paragraphe 2,

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 le service d'archivage électronique qualifié. La Commission doit établir une liste de normes de référence et, si nécessaire, des spécifications applicables à ces services.

(2) L'archivage électronique est un service qui assure la réception, le stockage, la récupération et la suppression de données électroniques et de documents électroniques afin d'en garantir la durabilité et la lisibilité, ainsi que d'en préserver l'intégrité, la confidentialité et la preuve de l'origine pendant toute la période de préservation. Les services d'archivage électronique 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. Pour faire en sorte que les données électroniques et les documents électroniques continuent à bénéficier d'une présomption quant à leur intégrité et à leur origine pendant la durée de la période de préservation par le prestataire de services de confiance qualifié, et pour atteindre un niveau élevé de transparence et de confiance entre tous les participants au cycle de vie de l'information, il est nécessaire d'établir un ensemble commun de spécifications applicables aux services d'archivage électronique qualifiés.

(3) Afin d'accroître la valeur probante, la sécurité et la fiabilité des services d'archivage électronique qualifiés, lorsque des signatures électroniques, des cachets électroniques ou des horodatages électroniques sont utilisés pour créer, par exemple, des preuves d'archivage, des enregistrements de preuves, des enregistrements d'événements, des enregistrements de la bonne mise en œuvre des procédures ou des rapports de confirmation d'archivage, pour les signer, les munir d'un cachet ou en attester la date et l'heure, il convient d'utiliser des services de confiance qualifiés.

(4) La présomption de conformité prévue à l'article 45 *undecies*, paragraphe 2, du règlement (UE) nº 910/2014 ne devrait s'appliquer que lorsque les prestataires de services d'archivage électronique qualifiés respectent les exigences énoncées dans le présent règlement. Les normes de référence applicables aux services d'archivage électronique qualifiés 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 des services d'archivage électronique qualifiés.

(5) Si un prestataire de services de confiance respecte les exigences énoncées par le 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.

(6) Afin de préserver l'intégrité et la preuve de l'origine des données électroniques et des documents électroniques contenant une ou plusieurs signatures ou un ou plusieurs cachets électroniques qualifiés, les services d'archivage électronique qualifiés devraient utiliser des procédures et des technologies permettant d'étendre la fiabilité de ces signatures ou cachets électroniques au-delà de la période de validité technologique et au moins pendant toute la période de préservation.

([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).

(7) 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.

(8) 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.

(9) 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 21 octobre 2025 ([6]).

(10) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Archivage électronique de documents portant une signature électronique qualifiée ou un cachet électronique qualifié

1. Lors de l'archivage de données électroniques ou de documents électroniques qui contiennent des signatures électroniques qualifiées ou des cachets électroniques qualifiés, les prestataires de services d'archivage électronique qualifiés veillent à ce que la fiabilité de ces signatures électroniques qualifiées ou cachets électroniques qualifiés soit préservée, y compris au-delà de leur période de validité technologique, et à ce que l'intégrité et l'exactitude de l'origine des signatures et cachets électroniques qualifiés soient préservées, au moins jusqu'à la fin de la période de préservation légale ou contractuelle.

2. Aux fins du paragraphe 1, les prestataires de services d'archivage électronique qualifiés peuvent s'appuyer sur un service qualifié de préservation des signatures électroniques qualifiées ou sur un service qualifié de préservation des cachets électroniques qualifiés.

Article 2

Normes de référence et spécifications applicables à la fourniture de services d'archivage électronique qualifiés

Les normes de référence et les spécifications mentionnées à l'article 45 *undecies*, paragraphe 2, du règlement (UE) nº 910/2014 figurent à l'annexe du présent règlement.

([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) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([6]) 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.

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 16 décembre 2025.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE

Liste des normes de référence et des spécifications applicables aux services d'archivage électronique qualifiés

La norme CEN/TS 18170:2025 («CEN/TS 18170») s'applique moyennant les adaptations suivantes:

a) Références normatives (clause 2)

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

— ETSI EN 319 421 V1.3.1 (2025-07) «Signatures électroniques et infrastructures (ESI) — Exigences de politique et de sécurité applicables aux prestataires de services de confiance délivrant des certificats».

— ISO 14721: 2025, Systèmes de transfert des informations et données spatiales — Système ouvert d'archivage d'information (SOAI) — Modèle de référence.

— 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).

— Règlement d'exécution (UE) 2024/482 de la Commission ([1]).

— Règlement d'exécution (UE) 2024/3144 de la Commission ([2]).

— 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».

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

b) Énoncé des pratiques et des politiques (paragraphe 6.1)

— Les exigences du paragraphe 6.1 de la norme CEN/TS 18170 s'appliquent.

— Les exigences du paragraphe 5 de la norme ETSI EN 319 401 s'appliquent.

— Le prestataire de service de confiance pour l'archivage électronique (EATSP) établit des procédures pour informer l'organe de contrôle de toute modification apportée à la fourniture du service de confiance pour l'archivage électronique et de l'intention de cesser ces activités, conformément aux exigences opérationnelles et aux dispositions législatives et réglementaires applicables, y compris conformément aux exigences des actes d'exécution adoptés en vertu de l'article 24, paragraphe 5, du règlement (UE) n° 910/2014 [i.2].

— L'EATSP informe l'organe de contrôle au moins:

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

  — trois mois avant la cessation prévue d'une prestation de services de confiance.

c) Termes et conditions (paragraphe 6.2)

— Les exigences du paragraphe 6.2 de la norme CEN/TS 18170 s'appliquent.

— Les abonnés et les parties utilisatrices du service de confiance pour l'archivage électronique reçoivent individuellement des informations claires, complètes et facilement accessibles, dans un espace accessible au public, relatives aux modalités et conditions précises, avant de nouer une relation contractuelle.

([1]) 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/oj).

([2]) 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).

d) Ressources humaines (paragraphe 7.3)

— Les exigences du paragraphe 7.3 de la norme CEN/TS 18170 s'appliquent.

— Le personnel de l'EATSP 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. 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.

e) Contrôles cryptographiques et surveillance (paragraphe 7.6)

— Le système d'archivage doit garantir la confidentialité des données et des documents pendant tout le cycle de vie de l'archive, du dépôt à l'élimination.

— Les exigences du paragraphe 7.5 «Contrôles cryptographiques» de la norme ETSI EN 319 401 s'appliquent.

— L'origine des données à archiver dans le système d'archivage électronique est établie par l'EATSP. Si des signatures ou des cachets électroniques sont utilisés à cette fin, ces signatures ou cachets doivent être qualifiés.

— Lorsque l'EATSP signe numériquement (une partie d') un objet ou d'un enregistrement numérique, la clé de signature privée de l'EATSP est conservée et utilisée soit dans un dispositif de création de signature ou de cachet électronique qualifié, soit 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 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 [règlements (UE) 2024/482 et (UE) 2024/3144] et certifié au niveau EAL 4 ou supérieur; ou

  c) jusqu'au 31.12.2030, à la norme FIPS PUB 140-3 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 [règlements (UE) 2024/482 et (UE) 2024/3144], ce dispositif est configuré et utilisé conformément à cette certification.

— L'EATSP contrôle la robustesse de l'algorithme cryptographique qui a été et est utilisé. Si l'un des algorithmes ou paramètres utilisés n'est plus jugé approprié au regard de la définition figurant dans la gestion des risques, l'EATSP met à jour la politique d'archivage correspondante ou crée un nouveau profil d'archivage pour traiter les AIP et définir et mettre en œuvre les mesures appropriées.

— L'évaluation des algorithmes cryptographiques et leur utilisation par l'EATSP sont conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA (ASM-ECCG).

— Les composants techniques de l'EATS s'authentifient mutuellement sur la base de techniques cryptographiques avant de communiquer.

f) Réseau (paragraphe 7.9)

— Les exigences du paragraphe 7.8 «Sécurité du réseau» de la norme ETSI EN 319 401 s'appliquent.

— L'analyse de vulnérabilité requise en vertu du REQ-7.8-13 de la norme ETSI EN 319 401 est effectuée au moins une fois par trimestre.

— Le test d'intrusion requis en vertu du REQ-7.8-17X de l'ETSI EN 319 401 est effectué au moins une fois par an.

— Les pare-feu sont configurés de manière à empêcher tous les protocoles et accès non nécessaires au fonctionnement de l'EATSP.

g) Collecte de preuves (paragraphe 7.11)

— Les exigences énoncées au paragraphe 7.10 «Collecte de preuves» de la norme ETSI EN 319 401, s'appliquent, y compris pour les événements critiques et non critiques (voir paragraphe 13.2).

h) Plan de résiliation et de résiliation de l'EATSP (paragraphe 7.13)

— Les exigences du paragraphe 7.13 de la norme CEN/TS 18170 s'appliquent.

— Le plan d'arrêt d'activité de l'EATSP 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) Fiabilité de l'heure des événements (paragraphe 13.3.1)

— Les exigences du paragraphe 13.3.1 de la norme CEN/TS 18170 s'appliquent.

— Lorsqu'il utilise des horodatages, l'EATSP utilise un horodatage qualifié.

Journal officiel
de l'Union européenne

FR
Série L

2026/248

3.2.2026

RÈGLEMENT D'EXÉCUTION (UE) 2026/248 DE LA COMMISSION

du 2 février 2026

portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne les formats des signatures électroniques avancées et des cachets électroniques avancés devant être reconnus par les organismes du secteur public, et abrogeant la décision d'exécution (UE) 2015/1506 de la Commission

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 27, paragraphe 5, et son article 37, paragraphe 5,

considérant ce qui suit:

(1) Les États membres doivent mettre en place les moyens techniques nécessaires au traitement des documents portant une signature ou un cachet électronique, qui sont requis pour utiliser un service en ligne offert par un organisme du secteur public ou en son nom.

(2) L'article 27 et l'article 37 du règlement (UE) nº 910/2014 prévoient que les États membres qui exigent une signature électronique avancée ou un cachet électronique avancé pour utiliser un service en ligne offert par un organisme du secteur public ou au nom de cet organisme reconnaissent les signatures électroniques avancées et les cachets électroniques avancés, les signatures électroniques avancées et les cachets électroniques avancés reposant sur un certificat qualifié et les signatures et les cachets électroniques qualifiés sous des formats spécifiques, ou sous d'autres formats validés conformément à des méthodes de référence données.

(3) Afin de faciliter la validation transfrontalière des signatures ou des cachets électroniques et d'améliorer l'interopérabilité transfrontalière des transactions électroniques, la décision d'exécution (UE) 2015/1506 de la Commission ([2]) a établi des formats de référence pour les signatures électroniques avancées et les cachets électroniques avancés devant être pris en charge par les États membres. Eu égard au développement de nouvelles technologies, pratiques, normes et spécifications techniques, il convient d'abroger la décision d'exécution (UE) 2015/1506. Le présent règlement d'exécution devrait fournir une liste de formats standard ainsi que les dispositions relatives à la reconnaissance de ces formats.

(4) Les formats standard figurant sur la liste devraient tenir compte des pratiques établies et être largement reconnus dans les secteurs concernés. Lorsqu'un format de signature électronique avancée ou de cachet électronique avancé autre que ceux dont la prise en charge technique est la plus courante est utilisé pour signer ou apposer un cachet, il convient de fournir des méthodes permettant la validation transfrontalière de ces signatures ou cachets électroniques avancés. Pour que les États membres destinataires puissent se fier aux méthodes de validation d'un autre État membre, l'État membre à l'origine de la transaction doit fournir des informations facilement accessibles sur ces méthodes. Par conséquent, il convient de faire figurer ces informations sur les méthodes de validation applicables dans les documents électroniques, dans les signatures électroniques avancées ou les cachets électroniques avancés, ou dans les conteneurs de documents électroniques.

(5) Lorsque d'autres méthodes de validation de cachets ou de signatures électroniques avancés adaptées au traitement automatisé sont disponibles dans les services publics d'un État membre, elles devraient être mises à la disposition de l'État membre destinataire et lui être fournies. Néanmoins, les dispositions de l'article 27, paragraphes 1 et 2, et de l'article 37, paragraphes 1 et 2, du règlement (UE) nº 910/2014 restent applicables lorsque le traitement automatisé d'autres méthodes de validation n'est pas techniquement possible.

([1]) JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Décision d'exécution (UE) 2015/1506 de la Commission du 8 septembre 2015 établissant les spécifications relatives aux formats des signatures électroniques avancées et des cachets électroniques avancés devant être reconnus par les organismes du secteur public visés à l'article 27, paragraphe 5, et à l'article 37, paragraphe 5, du règlement (UE) nº 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (JO L 235 du 9.9.2015, p. 37, ELI: http://data.europa.eu/eli/dec_impl/2015/1506/oj).

(6) Afin de fournir des exigences comparables pour la validation et de renforcer la confiance dans les méthodes de validation fournies par les États membres pour des formats de cachets ou de signatures électroniques avancés autres que ceux couramment pris en charge, les exigences relatives à ces méthodes de validation établies par le présent règlement découlent des exigences applicables à la validation des signatures et des cachets électroniques qualifiés énoncées aux articles 32 et 40 du règlement (UE) n° 910/2014, ainsi que des exigences applicables à la validation des signatures électroniques avancées et des cachets électroniques avancés reposant sur des certificats qualifiés énoncées à l'article 32 *bis* et à l'article 40 *bis* du règlement (UE) n° 910/2014.

(7) 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 ([3]), 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.

(8) Les États membres qui exigent une signature électronique avancée, une signature électronique avancée reposant sur un certificat qualifié, un cachet électronique avancé ou un cachet électronique avancé reposant sur un certificat qualifié, conformément à l'article 27, paragraphes 1 et 2, et à l'article 37, paragraphes 1 et 2, du règlement (UE) n° 910/2014, devraient reconnaître, respectivement, les signatures électroniques avancées utilisant des formats ou des conteneurs de signature associés, ou les cachets électroniques avancés utilisant des formats ou des conteneurs de cachet associés qui respectent les spécifications techniques énumérées dans le présent règlement. Cette obligation de reconnaissance des signatures électroniques avancées ou des cachets électroniques avancés lors de l'utilisation d'un service en ligne offert par un organisme du secteur public ou en son nom, devrait s'appliquer aussi longtemps que la validation des signatures électroniques avancées ou des cachets électroniques avancés sera requise par le droit de l'UE ou le droit national, à partir de leur création. Afin d'accorder aux États membres suffisamment de temps pour modifier leurs applications de validation, les exigences du présent règlement devraient devenir applicables 12 mois après l'entrée en vigueur du présent règlement. Pour assurer la transition vers les normes les plus récentes, l'obligation de reconnaître les signatures électroniques avancées ou les cachets électroniques avancés nouvellement créés aux formats standard énumérés dans la décision d'exécution (UE) 2015/1506 devrait être limitée dans le temps, jusqu'à 24 mois après l'entrée en vigueur du présent règlement.

(9) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([4]) et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([5]) s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du présent règlement.

(10) 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]).

(11) 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,

([3]) Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 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).

([4]) 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).

([5]) 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]) 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 draft Implementing Regulation on application of Regulation (EU) No 910/2014 regarding formats of advanced electronic signatures and seals to be recognised by public sector bodies and repealing Implementing Decision (EU) 2015/1506.

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Formats de signature électronique avancée

1. Les États membres qui exigent une signature électronique avancée ou une signature électronique avancée reposant sur un certificat qualifié, conformément à l'article 27, paragraphes 1 et 2, du règlement (UE) n° 910/2014, reconnaissent les signatures électroniques avancées utilisant un format ou un conteneur de signature associé qui respectent les spécifications techniques énumérées à l'annexe I du présent règlement.

2. Les États membres reconnaissent les signatures électroniques avancées utilisant un format ou un conteneur de signature associé qui respectent les spécifications techniques énumérées à l'annexe II du présent règlement, lorsque ces signatures électroniques ont été créées avant le 23 février 2028.

Article 2

Autres méthodes de validation de signatures électroniques avancées

1. Les États membres qui exigent une signature électronique avancée ou une signature électronique avancée reposant sur un certificat qualifié conformément à l'article 27, paragraphes 1 et 2, du règlement (UE) n° 910/2014, reconnaissent les formats de signatures électroniques avancées autres que ceux mentionnés à l'article 1er du présent règlement, lorsque:

a) l'État membre dans lequel le prestataire de services de confiance utilisé par le signataire est établi propose à d'autres États membres des méthodes de validation de signature pour ces formats; et que

b) ces méthodes de validation sont appliquées conformément au paragraphe 2.

2. Les méthodes de validation des autres formats de signature remplissent toutes les conditions suivantes:

a) elles sont, dans la mesure du possible, adaptées au traitement automatisé;

b) elles permettent à d'autres États membres de valider en ligne, gratuitement, la signature électronique reçue;

c) elles fournissent des instructions claires, complètes, facilement compréhensibles et accessibles pour procéder à la validation;

d) elles figurent dans le document signé, dans la signature électronique ou dans le conteneur de documents électroniques;

e) elles confirment la validité d'une signature électronique avancée, à condition que:

— le certificat qui prend en charge la signature électronique avancée ait été valide au moment de la signature,

— lorsque la signature électronique avancée est prise en charge par un certificat qualifié, ce certificat qualifié ait été, au moment de la signature, un certificat qualifié pour signature électronique conforme à l'annexe I du règlement (UE) n° 910/2014 et qu'il ait été établi par un prestataire de services de confiance qualifié,

— les données de validation de signature correspondent aux données transmises à la partie utilisatrice,

— l'ensemble unique de données représentant le signataire soit correctement fourni à la partie utilisatrice,

— si un pseudonyme a été utilisé au moment de la signature, la partie utilisatrice en ait été clairement informée,

— lorsque la signature électronique avancée est créée par un dispositif de création de signature électronique qualifié, l'utilisation d'un tel dispositif ait été clairement indiquée à la partie utilisatrice,

— l'intégrité des données signées n'ait pas été compromise,

— les exigences prévues à l'article 26 du règlement (UE) nº 910/2014 aient été respectées au moment de la signature,

— le système utilisé pour valider la signature électronique avancée fournisse à la partie utilisatrice le résultat correct du processus de validation et lui permette de détecter tout problème pertinent relatif à la sécurité.

3. Les informations visées au paragraphe 2, point d), permettent aux parties utilisatrices d'accéder facilement et gratuitement aux spécifications complètes de la méthode de validation de la signature.

Article 3

Formats de cachet électronique avancé

1. Les États membres qui exigent un cachet électronique avancé ou un cachet électronique avancé reposant sur un certificat qualifié conformément à l'article 37, paragraphes 1 et 2, du règlement (UE) nº 910/2014, reconnaissent les cachets électroniques avancés utilisant des formats ou des conteneurs de cachet associés qui respectent les spécifications techniques énumérées à l'annexe I du présent règlement.

2. Les États membres reconnaissent les cachets électroniques avancés utilisant des formats ou des conteneurs de cachets associés qui respectent les spécifications techniques énumérées à l'annexe II du présent règlement lorsque ces cachets électroniques ont été créés avant le 23 février 2028.

Article 4

Autres méthodes de validation de cachets électroniques avancés

1. Les États membres qui exigent un cachet électronique avancé ou un cachet électronique avancé reposant sur un certificat qualifié conformément à l'article 37, paragraphes 1 et 2, du règlement (UE) nº 910/2014, reconnaissent les formats de cachets électroniques autres que ceux mentionnés à l'article 3 du présent règlement, lorsque:

a) l'État membre dans lequel le prestataire de services de confiance utilisé par le créateur du cachet est établi propose à d'autres États membres des méthodes de validation de cachet pour ces formats; et que

b) ces méthodes de validation sont appliquées conformément au paragraphe 2.

2. Les méthodes de validation des autres formats de cachet remplissent toutes les conditions suivantes:

a) elles sont, dans la mesure du possible, adaptées au traitement automatisé;

b) elles permettent à d'autres États membres de valider en ligne, gratuitement, le cachet électronique reçu;

c) elles fournissent des instructions claires, complètes, facilement compréhensibles et accessibles pour procéder à la validation;

d) elles figurent dans le document portant le cachet, dans le cachet électronique ou dans le conteneur de documents électroniques; et

e) elles confirment la validité d'un cachet électronique avancé, à condition que:

— le certificat qui prend en charge le cachet électronique avancé ait été valide au moment de l'apposition du cachet,

— lorsque le cachet électronique avancé est pris en charge par un certificat qualifié, ce certificat qualifié ait été, au moment de l'apposition du cachet, un certificat qualifié pour cachet électronique conforme à l'annexe III du règlement (UE) nº 910/2014 et qu'il ait été établi par un prestataire de services de confiance qualifié,

— les données de validation du cachet correspondent aux données communiquées à la partie utilisatrice,

— l'ensemble unique de données représentant le créateur du cachet soit correctement fourni à la partie utilisatrice,

— si un pseudonyme a été utilisé au moment de l'apposition du cachet, la partie utilisatrice en ait été clairement informée,

— lorsque le cachet électronique avancé est créé par un dispositif de création de cachet électronique qualifié, l'utilisation d'un tel dispositif ait été clairement indiquée à la partie utilisatrice,

— l'intégrité des données portant le cachet n'ait pas été compromise,

— les exigences prévues à l'article 36 du règlement (UE) n° 910/2014 aient été satisfaites au moment de l'apposition du cachet, et que

— le système utilisé pour valider le cachet électronique avancé fournisse à la partie utilisatrice le résultat correct du processus de validation et permette à celle-ci de détecter tout problème pertinent relatif à la sécurité.

3. Les informations visées au paragraphe 2, point d), permettent aux parties utilisatrices d'accéder facilement et gratuitement aux spécifications complètes de la méthode de validation du cachet.

Article 5

Abrogation

La décision d'exécution (UE) 2015/1506 est abrogée.

Les références à la décision abrogée s'entendent comme faites au présent règlement.

Article 6

Entrée en vigueur

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

L'article 1er, paragraphe 1, et l'article 3, paragraphe 1, sont applicables à partir du 23 février 2027.

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

Fait à Bruxelles, le 2 février 2026.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE I

Liste des spécifications techniques applicables aux signatures électroniques avancées visées à l'article 1er, paragraphe 1, et aux cachets électroniques avancés visés à l'article 3, paragraphe 1

XAdES Baseline Profile	ETSI EN 319 132-1 V1.3.1 (2024-07) (1)
CAdES Baseline Profile	ETSI EN 319 122-1 V1.3.1 (2023-06) (2)
PAdES Baseline Profile	ETSI EN 319 142-1 V1.2.1 (2024-01) (3)
JAdES Baseline Profile	ETSI TS 119 182-1 V1.2.1 (2024-07) (4), moyennant l'adaptation suivante: — le paragraphe 5.1.8 intitulé «Le paramètre d'en-tête x5c (Chaîne de certificat X.509)» est remplacé par le texte suivant: «5.1.8 **Le paramètre d'en-tête x5c (Chaîne de certificat X.509)** Le paramètre d'en-tête x5c tel que défini dans le paragraphe 4.1.6 de la RFC 7515 de l'IETF [2] doit être présent dans la signature JAdES, sous la forme d'un paramètre d'en-tête signé ou non signé. Le paramètre d'en-tête x5c doit avoir la sémantique spécifiée dans la RFC 7515 de l'IETF, paragraphe 4.1.6. Le paramètre d'en-tête x5c doit avoir la syntaxe spécifiée dans la RFC 7515 de l'IETF, paragraphe 4.1.6.»

(1) https://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.03.01_60/en_31913201v010301p.pdf.
(2) https://www.etsi.org/deliver/etsi_en/319100_319199/31912201/01.03.01_60/en_31912201v010301p.pdf.
(3) https://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.02.01_60/en_31914201v010201p.pdf.
(4) https://www.etsi.org/deliver/etsi_ts/119100_119199/11918201/01.02.01_60/ts_11918201v010201p.pdf.

Liste des spécifications techniques applicables aux conteneurs de signature associés visés à l'article 1er, paragraphe 1, et aux conteneurs de cachet associés visés à l'article 3, paragraphe 1

Associated Signature/Seal Container Baseline Profile	ETSI EN 319 162-1 V1.1.1 (2016-04) (1) ETSI EN 319 162-2 V1.1.1 (2016-04) (2) pour le conteneur supplémentaire ASiC-E CAdES; tel que spécifié au paragraphe 4.3.1.

(1) https://www.etsi.org/deliver/etsi_en/319100_319199/31916201/01.01.01_60/en_31916201v010101p.pdf.
(2) https://www.etsi.org/deliver/etsi_en/319100_319199/31916202/01.01.01_60/en_31916202v010101p.pdf.

ANNEXE II

Liste des spécifications techniques applicables aux signatures électroniques avancées visés à l'article 1er, paragraphe 2, et aux cachets électroniques avancés visés à l'article 3, paragraphe 2

XAdES Baseline Profile	ETSI TS 103 171 v.2.1.1 ([1]), à l'exception du paragraphe 9 et au niveau de conformité B, T ou LT
CAdES Baseline Profile	ETSI TS 103 173 v.2.2.1 ([2]), à l'exception du paragraphe 9 et au niveau de conformité B, T ou LT
PAdES Baseline Profile	ETSI TS 103 172 v.2.2.2 ([3]), à l'exception du paragraphe 9 et au niveau de conformité B, T ou LT

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf.
([2]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf.
([3]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf.

Liste des spécifications techniques applicables aux conteneurs de signature associés visés à l'article 1er, paragraphe 2, et aux conteneurs de cachet associés visés à l'article 3, paragraphe 2

Associated Signature/Seal Container Baseline Profile	ETSI TS 103 174 v.2.2.1 ([1])

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf.

Journal officiel
de l'Union européenne

FR
Série L

2026/798

8.4.2026

RÈGLEMENT D'EXÉCUTION (UE) 2026/798 DE LA COMMISSION

du 7 avril 2026

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 à l'enrôlement à distance des utilisateurs pour les portefeuilles européens d'identité numérique par des moyens d'identification électronique conformes au niveau de garantie substantiel combinés avec des procédures d'enrôlement à distance supplémentaires lorsque la combinaison répond aux exigences du niveau de garantie élevé

LA COMMISSION 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 5 *bis*, paragraphe 24,

considérant ce qui suit:

(1) L'enrôlement des utilisateurs pour les portefeuilles européens d'identité numérique (ci-après les «portefeuilles») est une étape essentielle dans la vérification de l'identité des utilisateurs de portefeuille et l'établissement du lien entre les données d'identification personnelle des utilisateurs et leur portefeuille et le dispositif utilisateur sur lequel les unités de portefeuille sont installées.

(2) Afin de favoriser un niveau élevé de confiance et de sécurité ainsi qu'une approche harmonisée dans l'ensemble des États membres pour l'enrôlement des utilisateurs de portefeuille par des procédures d'enrôlement à distance combinées avec les moyens d'identification électronique conformes au niveau de garantie substantiel, le présent acte d'exécution établit des spécifications et des procédures afin de faciliter l'enrôlement des utilisateurs pour le portefeuille européen d'identité numérique par des moyens d'identification électronique conformes au niveau de garantie substantiel combinés avec des procédures d'enrôlement à distance supplémentaires qui, conjointement, répondent aux exigences du niveau de garantie élevé.

(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 exigences qui garantissent la sécurité et la fiabilité de l'enrôlement des utilisateurs.

(4) Le règlement d'exécution (UE) 2015/1502 de la Commission ([2]) dispose que, lorsque des moyens d'identification électronique sont délivrés au niveau de garantie élevé, et en tenant compte des risques d'une modification des données d'identification personnelle, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité. Par conséquent, en pareil cas, les États membres devraient se servir de moyens d'identification électronique délivrés au niveau de garantie élevé pour les appliquer également au processus d'enrôlement aux fins du présent règlement.

(5) Lorsque les États membres enrôlent des utilisateurs pour des portefeuilles par un moyen d'identification électronique qui n'a pas été notifié à la Commission, le niveau de garantie de ce moyen devrait être confirmé par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 du Parlement européen et du Conseil ([3]) ou par un organisme équivalent et il devrait être démontré que les résultats de cette procédure de délivrance antérieure d'un moyen d'identification électronique restent valables.

([1]) JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) nº 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (JO L 235 du 9.9.2015, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([3]) Règlement (CE) nº 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) nº 339/93 du Conseil (JO L 218 du 13.8.2008, p. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

(6) Bien que l'annexe énonce les exigences à remplir pour atteindre un niveau spécifique de preuve d'identité, l'équivalence n'a pas été établie en ce qui concerne les niveaux de garantie définis à l'article 8 du règlement (UE) nº 910/2014. Par conséquent, les exigences énoncées dans l'annexe devraient être considérées comme mettant en œuvre celles du règlement d'exécution (UE) 2015/1502 et devant être remplies par le fournisseur de données d'identification personnelle ou une entité fournissant des services de preuve d'identité pour le compte de ce fournisseur.

(7) La Commission évalue régulièrement les nouvelles technologies, pratiques et spécifications techniques. Conformément au considérant 75 du règlement (UE) 2024/1183 du Parlement européen et du Conseil ([4]), 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 et les nouvelles technologies, normes ou spécifications techniques et de suivre les meilleures pratiques sur le marché intérieur, en particulier quant à l'enrôlement des utilisateurs pour le portefeuille.

(8) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([5]) ainsi que, le cas échéant, le règlement (UE) 2018/1725 du Parlement européen et du Conseil ([6]) et la directive 2002/58/CE du Parlement européen et du Conseil ([7]) s'appliquent aux activités de traitement de données à caractère personnel au titre du présent règlement.

(9) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 et a rendu son avis le 30 janvier 2026 ([8]).

(10) Le comité institué par l'article 48 du règlement (UE) nº 910/2014 n'a pas émis d'avis dans le délai fixé par sa présidence,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Les normes de référence et les spécifications mentionnées à l'article 5 *bis*, paragraphe 24, du règlement (UE) nº 910/2014 figurent à l'annexe du présent règlement.

([4]) 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).

([5]) 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).

([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) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) 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).

([8]) EDPS Formal comments on the draft Commission Implementing Regulation as regards onboarding of users to the European Digital Identity Wallets.

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 7 avril 2026.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE

LISTE DES NORMES DE RÉFÉRENCE ET SPÉCIFICATIONS

La conformité est évaluée au regard des clauses de la norme ETSI TS 119 461 V2.1.1 (2025-02) énumérées à la section 1, sous réserve des adaptations énumérées à la section 2.

Section 1 — Clauses applicables

—	5	Évaluation du risque opérationnel
—	6	Politiques et méthodes
—	7	Gestion et exploitation du service de preuve de l'identité
—	8	Exigences du service de preuve de l'identité
—	9.1	Introduction, conformité avec le présent document, exigences générales pour tous les cas d'utilisation
—	9.2.2	Cas d'utilisation à partir d'un document d'identité pour la preuve de l'identité à distance non automatisée
—	9.2.3	Cas d'utilisation à partir d'un document d'identité pour la preuve de l'identité à distance automatisée
—	9.2.4	Cas d'utilisation pour la preuve de l'identité par authentification à partir de moyens d'identification électronique
—	9.5	Cas d'utilisation pour une preuve d'identité supplémentaire visant à renforcer une identité prouvée au moyen d'une identification électronique à partir du niveau Baseline LoIP vers le niveau Extended LoIP.

Section 2 — Adaptations

1.	5	Évaluation du risque opérationnel
	—	OVR-5-01: Les exigences spécifiées dans l'ETSI EN 319 401 [1], clause 5, doivent s'appliquer.
	—	*Note 1*: Lorsque la preuve de l'identité est effectuée par le fournisseur de données d'identification personnelle lui-même, l'évaluation des risques du fournisseur de données d'identification personnelle peut couvrir la preuve de l'identité.
2.	6.1	Énoncé des pratiques du service de preuve d'identité
	—	OVR-6.1-02: Un IPSP identifie dans son énoncé des pratiques les cas d'utilisation pour lesquels la conformité avec le présent document est alléguée.
	—	*Note 1:* Lorsque la preuve de l'identité est effectuée par le fournisseur de données d'identification personnelle lui-même, l'énoncé des pratiques du service de preuve d'identité du fournisseur de données d'identification personnelle peut couvrir les informations relatives à la preuve d'identité et il n'est pas nécessaire d'établir d'énoncé des pratiques spécifique pour la preuve d'identité.
3.	7.9	Vulnérabilités et gestion des incidents
	—	OVR-7.9-02: Les obligations de déclaration conformément à la norme ETSI EN 319401 [1] REQ-7.9.2-02X et à la clause 7.9.3 doivent être remplies en fonction du contexte d'établissement de la preuve d'identité et des obligations du fournisseur de données d'identification personnelle dépendant du service de l'IPSP.
	—	Exemple: Les déclarations à l'autorité de contrôle chargée de la surveillance d'un fournisseur de portefeuilles européens d'identité numérique établi dans l'État membre qui a procédé à la désignation peuvent être effectuées en coopération entre l'IPSP et le fournisseur de données d'identification personnelle.

4. 7.10 Collecte d'éléments de preuve

— OVR-7.10-01: Les exigences spécifiées dans l'ETSI EN 319401 [1], clause 7.10, doivent s'appliquer.

— *Note 1:* Les exigences à long terme en matière de conservation des éléments de preuve peuvent être remplies par le fournisseur de données d'identification personnelle demandant la preuve d'identité plutôt que par l'IPSP lorsque les deux entités sont différentes.

— *Note 2:* Les exigences de la clause 8.5.2 du présent document s'appliquent.

5. 7.11 Gestion de la continuité des activités

— OVR-7.11-02: Les processus de gestion de crises conformément à la norme ETSI EN 319401 [1], REQ-7.11.3-01X doivent être tels que le requièrent le contexte d'établissement de la preuve d'identité et les obligations du fournisseur de données d'identification personnelle dépendant du service de l'IPSP.

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

— OVR-7.12-01: Les exigences spécifiées dans la norme ETSI EN 319401 [1], clause 7.12, à l'exclusion de REQ-7.12-11, doivent s'appliquer.

— *Note:* Lorsque l'IPSP et le fournisseur de données d'identification personnelle demandant la preuve d'identité sont des entités différentes, ils peuvent convenir d'une assistance mutuelle ou unilatérale pour l'établissement des plans d'arrêt d'activité.

7. 8.1 Initiation

— INI-8.1-05: En cas d'interruption ou d'échec du processus de preuve d'identité à distance, l'IPSP doit veiller à ce que des explications et des possibilités de solution suffisantes soient fournies aux personnes, en particulier dans le cadre de la preuve d'identité à distance automatisée. Les informations devraient permettre aux personnes concernées de contribuer efficacement à la résolution rapide du problème et, si nécessaire, d'exercer leurs droits (tels que le droit de rectification ou la possibilité de contester la décision) à l'encontre du responsable du traitement concerné.

8. 8.2.1 Exigences générales

— COL-8.2.1-08: L'IPSP doit mettre en œuvre des mesures visant à garantir le respect des exigences en matière de protection des données dès la conception et par défaut conformément à l'article 25 du règlement (UE) 2016/679 au cours du processus d'enrôlement, en particulier en ce qui concerne le traitement des données biométriques. Les mesures en question peuvent comprendre, selon le cas, des contrôles cryptographiques, des dispositifs et des mesures organisationnelles de nature à renforcer la protection de la vie privée. Ces mesures devraient limiter la collecte de données à ce qui est strictement nécessaire au traitement des données biométriques et de toute autre donnée à caractère personnel à recueillir auprès des sources d'identification physiques et numériques en vue de relier les données d'identification personnelle de l'utilisateur à son portefeuille et à l'appareil de l'utilisateur sur lequel l'unité de portefeuille est installée.

9. 8.2.4 Utilisation de moyens d'identification électronique existants à titre d'élément de preuve

— [CONDITIONNEL] COL-8.2.4-02X: Si le niveau Baseline LoIP est visé, le moyen d'identification électronique doit avoir été notifié au moins au niveau de garantie substantiel d'eIDAS ou son niveau de garantie doit avoir été confirmé par un organisme d'évaluation de la conformité accrédité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou par un organisme équivalent et, si toutes les exigences applicables sont remplies, l'évaluation doit donner lieu 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 pour les portefeuilles européens d'identité numérique certifiés au titre du règlement (UE) nº 910/2014 [i.25].

— COL-8.2.4-02A: néant.

10. 8.3.1 Exigences générales

— VAL-8.3.1-11X: Le processus de preuve de l'identité vérifie que les éléments de preuve sont valables au moment de l'établissement de la preuve d'identité.

11. 8.3.3 Validation du document d'identité physique

— VAL-8.3.3-21: 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 doit être confirmée par un organisme d'évaluation de la conformité accrédité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou un organisme équivalent.

— VAL-8.3.3-22: L'image faciale de référence du document d'identité physique est recueillie par communication en champ proche et le processus assure l'authentification passive ou active de la puce sur le document d'identité physique.

12. 9.1 Introduction, conformité avec le présent document, exigences générales pour tous les cas d'utilisation

— USE-9.1-01X: Pour être conforme au présent document, un processus de preuve d'identité doit être conforme au cas d'utilisation figurant à la clause 9.5 du présent document pour le niveau Extended LoIP.

— USE-9.1-03X: néant.

13. 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. Les valeurs cibles utilisées par l'IPSP 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.

14. 9.5.1 Exigences générales

— Premier alinéa: Lorsque le demandeur est une personne physique, y compris une personne physique représentant une personne morale, que l'identité du demandeur a été prouvée au niveau Baseline LoIP par authentification à partir de moyens d'identification électronique et qu'un renforcement au niveau Extended LoIP est nécessaire, les exigences suivantes s'appliquent.

— USE-9.5.1-08: La preuve d'identité supplémentaire requise pour renforcer la fiabilité d'une identité ne s'applique qu'à l'identification électronique qui n'a pas été délivrée en recourant à une comparaison automatisée entre des images faciales pour le processus de délivrance initial.

15. 9.5.2 Cas d'utilisation pour le renforcement de la preuve d'identité au niveau Extended LoIP par l'établissement d'une preuve d'identité complète à partir d'un document d'identité

— USE-9.5.2-01: La preuve d'identité visant à passer du niveau Baseline LoIP au niveau Extended LoIP doit être conforme aux exigences applicables au niveau Extended LoIP dans l'un des cas d'utilisation décrits dans les clauses 9.2.2 ou 9.2.3 du présent document pour le niveau Extended LoIP.

16. 9.5.3 Cas d'utilisation pour le renforcement de la preuve d'identité au niveau Extended LoIP au moyen d'une image faciale de référence précédemment saisie

— USE-9.5.3-01: Un processus de preuve de l'identité satisfaisant aux exigences du niveau Extended LoIP dans l'un des cas d'utilisation décrits dans les clauses 9.2.2 ou 9.2.3 du présent document ou un processus de preuve de l'identité ayant fait l'objet d'un examen par les pairs ou ayant été certifié par un organisme d'évaluation de la conformité accrédité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou un organisme équivalent afin d'assurer un niveau de garantie élevé conformément au règlement (UE) nº 910/2014 [i.25] doit être utilisé pour saisir une image faciale de référence et lier les attributs d'identité nécessaires à cette image faciale de référence.

Journal officiel
de l'Union européenne

FR
Série L

2026/1730

22.7.2026

RÈGLEMENT D'EXÉCUTION (UE) 2026/1730 DE LA COMMISSION

du 15 juillet 2026

modifiant le règlement d'exécution (UE) 2025/848 en ce qui concerne les normes et spécifications applicables

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 5 *ter*, paragraphe 11,

considérant ce qui suit:

(1) Afin de garantir le niveau d'harmonisation le plus élevé possible entre les États membres pour le développement des portefeuilles européens d'identité numérique, les spécifications techniques applicables aux portefeuilles s'appuient sur les travaux réalisés sur la base de la recommandation (UE) 2021/946 de la Commission ([2]) et, en particulier, sur l'architecture et le cadre de référence. Étant donné que l'architecture et le cadre de référence ont considérablement évolué depuis l'adoption du règlement d'exécution (UE) 2025/848 de la Commission ([3]), il convient à présent de modifier ledit règlement d'exécution afin de l'aligner sur les nouvelles normes, spécifications et procédures. En outre, afin de favoriser l'interopérabilité entre les registres des parties utilisatrices de portefeuille, les spécifications techniques pertinentes applicables à un format commun et à une interface de programmation d'application (API) commune pour les informations relatives à l'enregistrement des parties utilisatrices de portefeuille ont été élaborées dans le cadre de l'architecture et du cadre de référence.

(2) Conformément aux objectifs du règlement (UE) nº 910/2014, un certain nombre de normes ont été sélectionnées pour satisfaire aux exigences applicables à l'enregistrement des parties utilisatrices de portefeuille. Ces normes devraient tenir compte des pratiques établies et être largement reconnues dans les secteurs concernés. Si nécessaire, ces normes devraient être adaptées ou complétées afin de garantir un niveau élevé de sécurité et de fiabilité dans l'enregistrement et l'identification des parties utilisatrices de portefeuille, tout en facilitant l'interopérabilité transfrontière et le bon fonctionnement du marché intérieur. Conformément à cet objectif, le présent règlement met à jour les normes techniques et les exigences en matière d'information applicables à l'enregistrement du lien entre les intermédiaires et les parties utilisatrices de portefeuille pour le compte desquelles ils agissent et harmonise les profils de certificat pour les certificats régis par le présent règlement.

(3) Afin de permettre à l'unité de portefeuille de confirmer que les données demandées par une partie utilisatrice de portefeuille relèvent du champ d'application de l'utilisation prévue enregistrée, les fournisseurs de certificats d'enregistrement de partie utilisatrice de portefeuille devraient délivrer les certificats d'enregistrement de partie utilisatrice de portefeuille de manière automatisée et sans retard injustifié après l'enregistrement.

([1]) JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Recommandation (UE) 2021/946 de la Commission du 3 juin 2021 concernant une boîte à outils commune de l'Union pour une approche coordonnée en vue d'un cadre européen relatif à une identité numérique (JO L 210 du 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reg/2021/946/oj).

([3]) Règlement d'exécution (UE) 2025/848 de la Commission du 6 mai 2025 portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne l'enregistrement des parties utilisatrices de portefeuilles (JO L, 2025/848, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/848/oj).

(4) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([4]) et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([5]) s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du présent règlement.

(5) 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 17 avril 2026 ([7]).

(6) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Modification du règlement d'exécution (UE) 2025/848

Le règlement d'exécution (UE) 2025/848 est modifié comme suit:

1) À l'article 6, paragraphe 3, le point a) est remplacé par le texte suivant:

«a) l'exactitude, la validité, l'authenticité et l'intégrité des informations requises en vertu de l'annexe I, points 1 à 6 et 11 à 16;».

2) À l'article 6, paragraphe 3, le point c) est supprimé.

3) À l'article 6, le paragraphe 3 *bis* suivant est inséré:

«3 *bis*.Les bureaux d'enregistrement recueillent les informations visées à l'annexe I, points 7 à 10, de manière automatisée uniquement à des fins de transparence et, sans préjudice de l'article 5 *ter*, paragraphe 4, du règlement (UE) nº 910/2014, n'appliquent aucune procédure d'autorisation préalable à ces informations.».

4) L'article 8 est modifié comme suit:

a) le paragraphe 1 est remplacé par le texte suivant:

«1. Les États membres autorisent au moins une autorité de certification à délivrer des certificats d'enregistrement de partie utilisatrice de portefeuille. Les États membres veillent à ce que les fournisseurs de certificats d'enregistrement de partie utilisatrice de portefeuille délivrent ces certificats de manière automatisée et sans retard injustifié après l'enregistrement.»;

b) le paragraphe 2 est remplacé par le texte suivant:

«2. Les États membres:

a) imposent aux fournisseurs de certificats d'enregistrement de partie utilisatrice de portefeuille l'obligation de délivrer lesdits certificats aux seules parties utilisatrices de portefeuille enregistrées;

b) veillent à ce que chaque utilisation prévue soit exprimée dans les certificats d'enregistrement de partie utilisatrice de portefeuille;

([4]) Règlement (UE) 2016/679 du Parlement 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).

([5]) 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]) 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) nº 45/2001 et la décision nº 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 amending Implementing Regulation (EU) 2025/848 as regards applicable standards and specifications. [Commentaires formels du CEPD sur le projet de règlement d'exécution modifiant le règlement d'exécution (UE) 2025/848 en ce qui concerne les normes et spécifications applicables]. | Contrôleur européen de la protection des données.

c) veillent à ce que les certificats d'enregistrement de partie utilisatrice de portefeuille comportent une politique d'accès générale, dont l'harmonisation syntaxique et sémantique est assurée dans l'ensemble de l'Union, informant les utilisateurs que la partie utilisatrice de portefeuille est uniquement autorisée à demander les données spécifiées dans les certificats d'enregistrement pour l'utilisation prévue enregistrée dans lesdits certificats;

d) veillent à ce que les fournisseurs de solutions de portefeuille établis dans cet État membre se conforment à la politique d'accès générale en informant les utilisateurs lorsqu'une partie utilisatrice de portefeuille demande des données qui ne figurent pas dans les certificats d'enregistrement;

e) mettent en œuvre les certificats d'enregistrement de partie utilisatrice de portefeuille en assurant leur harmonisation syntaxique et sémantique et dans le respect des exigences énoncées à l'annexe V;

f) mettent en œuvre des politiques en matière de certificats et des énoncés des pratiques de certification spécifiques pour les certificats d'enregistrement de partie utilisatrice de portefeuille, conformément aux exigences énoncées à l'annexe V;

g) veillent à ce que les parties utilisatrices de portefeuille fournissent un URL pour la politique en matière de protection de la vie privée concernant l'utilisation prévue.».

5) L'annexe I est modifiée conformément à l'annexe I du présent règlement.

6) L'annexe IV est modifiée conformément à l'annexe II du présent règlement.

7) L'annexe V est modifiée conformément à l'annexe III 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 15 juillet 2026.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE I

À l'annexe I du règlement d'exécution (UE) 2025/848, le point suivant est ajouté:

«16. Le cas échéant, un lien d'association avec la partie utilisatrice de portefeuille qui recourt à l'intermédiaire auquel le certificat d'accès de partie utilisatrice de portefeuille a été délivré et qui agit pour le compte de la partie utilisatrice qui a l'intention de se fier au portefeuille.».

ANNEXE II

L'annexe IV du règlement d'exécution (UE) 2025/848 est modifiée comme suit:

1) au point 3, le premier alinéa est modifié comme suit:

   a) Le texte «sont, le cas échéant, au moins conformes aux exigences de la politique de certification normalisée énoncées dans la norme ETSI EN 319 411-1 version 1.4.1 (2023-10)» est remplacé par le texte «sont, le cas échéant, conformes à la norme ETSI TS 119 411-8 V1.1.1 (2025-10)»;

2) le point 3, k), est modifié comme suit:

   a) le troisième tiret est remplacé par le texte suivant:

      «— les informations visées à l'annexe I, points 1, 2, 3, 5, 6 et 7, a), b) et c), et 16;»;

   b) le quatrième tiret suivant est ajouté:

      «— une référence au registre national des parties utilisatrices de portefeuille dans lequel la partie utilisatrice est enregistrée.».

ANNEXE III

L'annexe V du règlement d'exécution (UE) 2025/848 est modifiée comme suit:

1) au point 3, le premier alinéa est modifié comme suit:

   a) le texte «sont au moins conformes aux exigences de la politique de certification normalisée énoncées dans la norme ETSI EN 319 411-1 version 1.4.1 (2023-10)» est remplacé par le texte «sont conformes à la norme ETSI TS 119 475 V1.2.1 (2026-03)»;

2) le point 3, j), est modifié comme suit:

   a) le cinquième tiret est remplacé par le texte suivant:

      «— inclure une politique d'accès générale au sens de l'article 8, paragraphe 2, point c).».

Journal officiel
de l'Union européenne

FR
Série L

2026/1731

22.7.2026

RÈGLEMENT D'EXÉCUTION (UE) 2026/1731 DE LA COMMISSION

du 15 juillet 2026

modifiant les règlements d'exécution (UE) 2024/2977, (UE) 2024/2979, (UE) 2024/2980 et (UE) 2024/2982 en ce qui concerne les normes et spécifications applicables

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 5 *bis*, paragraphe 23,

considérant ce qui suit:

(1) Afin de garantir le niveau d'harmonisation le plus élevé possible entre les États membres pour le développement des portefeuilles européens d'identité numérique, les spécifications techniques applicables aux portefeuilles s'appuient sur les travaux réalisés sur la base de la recommandation (UE) 2021/946 de la Commission ([2]) et, en particulier, sur l'architecture et le cadre de référence. Étant donné que l'architecture et le cadre de référence ont considérablement évolué depuis les règlements d'exécution (UE) 2024/2977 ([3]), (UE) 2024/2979 ([4]), (UE) 2024/2980 ([5]) et (UE) 2024/2982 ([6]) de la Commission, il convient à présent de modifier ces règlements d'exécution afin de les aligner sur les nouvelles normes, spécifications et procédures.

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. Par exemple, étant donné que le format VCDM du W3C est utilisé comme format de référence pour les attestations, en particulier dans le secteur de l'éducation, les portefeuilles européens d'identité numérique devraient également prendre en charge ce format lorsque les nouveaux profils au format VCDM du W3C seront disponibles. Si nécessaire, ces normes devraient être adaptées ou complétées afin de garantir la sécurité et la fiabilité des portefeuilles européens d'identité numérique, tout en facilitant l'interopérabilité transfrontière et le bon fonctionnement du marché intérieur.

(2) Pour toute utilisation du portefeuille qui nécessite la présentation du portrait de l'utilisateur de portefeuille, les solutions de portefeuille doivent prendre en charge la fonctionnalité de divulgation sélective et l'utilisateur doit conserver le contrôle total de la divulgation. Afin de préserver la faculté de décider de la divulgation et de protéger le portrait contre une demande de divulgation non intentionnelle ou non autorisée, la conception architecturale des portefeuilles européens d'identité numérique devrait prévoir des mécanismes d'avertissement ainsi que la journalisation de toutes les transactions relatives à l'utilisation du portrait. Pour que l'utilisateur de portefeuille soit conscient qu'il partage des données biométriques, les messages d'avertissement devraient indiquer que la demande

([1]) JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Recommandation (UE) 2021/946 de la Commission du 3 juin 2021 concernant une boîte à outils commune de l'Union pour une approche coordonnée en vue d'un cadre européen relatif à une identité numérique (JO L 210 du 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reg/2021/946/oj).
([3]) Règlement d'exécution (UE) 2024/2977 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne les données d'identification personnelle et les attestations électroniques d'attributs délivrées aux portefeuilles européens d'identité numérique (JO L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).
([4]) Règlement d'exécution (UE) 2024/2979 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne l'intégrité et les fonctionnalités essentielles des portefeuilles européens d'identité numérique (JO L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).
([5]) Règlement d'exécution (UE) 2024/2980 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne les notifications relatives à l'écosystème des portefeuilles européens d'identité numérique transmises à la Commission (JO L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).
([6]) Règlement d'exécution (UE) 2024/2982 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en ce qui concerne les protocoles et les interfaces que doit prendre en charge le cadre européen relatif à une identité numérique (JO L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

implique le partage de données biométriques et exiger expressément que la divulgation soit confirmée par l'utilisateur. Lorsqu'une partie utilisatrice traite le portrait aux fins d'identifier une personne physique de manière unique ou de confirmer l'identité déclarée de cette personne, les articles 6 et 9 du règlement (UE) 2016/679 du Parlement européen et du Conseil ([7]) s'appliquent, ainsi que toutes les autres exigences dudit règlement, notamment en ce qui concerne la limitation du traitement du portrait à ce qui est nécessaire à l'utilisation prévue. L'utilisation prévue, ainsi que la demande de divulgation, devraient être communiquées à l'utilisateur de portefeuille dans un langage clair et intelligible. Afin de tenir dûment compte de la sensibilité des données biométriques, il convient que l'utilisateur de portefeuille confirme explicitement et expressément la divulgation. Ni l'absence de réponse ni des cases cochées par défaut ne devraient avoir valeur de confirmation par l'utilisateur de portefeuille. La confirmation explicite de l'utilisateur de portefeuille devrait être une garantie technique et ne devrait pas constituer en soi un fondement juridique pour le traitement. Comme le prévoit l'article 9, paragraphe 4, du règlement (UE) 2016/679, les États membres peuvent maintenir ou instaurer des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement de données génétiques, biométriques, ou de données concernant la santé.

(3) Afin de laisser aux États membres suffisamment de temps pour adapter leurs procédures nationales, le portrait de l'utilisateur de portefeuille peut ne faire partie des données d'identification personnelle obligatoires pour la personne physique qu'à partir du 11 août 2028. Lorsque ces images proviennent de documents d'identité existants, tels que des cartes d'identité ou des passeports, les exigences pertinentes énoncées respectivement dans le règlement (UE) 2025/1208 ([8]) ou le règlement (CE) n° 2252/2004 ([9]) du Conseil s'appliquent.

(4) Le règlement (UE) n° 910/2014 exige que les portefeuilles puissent afficher un label de confiance de l'UE pour le portefeuille d'identité numérique, indiquant de manière vérifiable, simple et reconnaissable qu'un portefeuille a été fourni conformément au règlement. L'utilisation de ce label de confiance contribuera au bon fonctionnement du marché intérieur, garantira une concurrence loyale et protégera les intérêts des consommateurs. Pour permettre l'utilisation de ce label, il convient d'en établir les caractéristiques visuelles et techniques.

(5) Comme le prévoit l'article 12 *ter* du règlement (UE) n° 910/2014, les contrôleurs d'accès doivent permettre aux fournisseurs de portefeuilles européens d'identité numérique et aux émetteurs de moyens d'identification électronique notifiés d'interopérer effectivement avec le même système d'exploitation, les mêmes caractéristiques matérielles et logicielles et, aux fins de l'interopérabilité, d'accéder effectivement à ce même système et à ces mêmes caractéristiques. Cette interopérabilité et cet accès effectifs sont permis gratuitement, et ce, que ces caractéristiques matérielles ou logicielles fassent partie ou non du système d'exploitation, qu'elles soient disponibles ou non pour ce contrôleur d'accès ou qu'elles soient utilisées ou non par ce contrôleur d'accès dans le cadre de la fourniture de tels services. Étant donné que toutes les solutions de portefeuille devraient prendre en charge un ensemble commun de protocoles et d'interfaces afin de garantir la facilité d'utilisation, la sécurité et l'interopérabilité dans tous les États membres, les contrôleurs d'accès devraient activer le système d'exploitation et les caractéristiques matérielles ou logicielles nécessaires à la mise en œuvre des protocoles et interfaces énoncés à l'annexe XII du présent règlement. De ce fait, dans les flux en ligne multi-appareils, tant pour la vérification de proximité physique que pour le transfert de données entre les deux appareils, les contrôleurs d'accès devraient privilégier l'utilisation d'un canal de communication locale tel que prévu par la version 2.3 de la spécification de protocole client-authentificateur (CTAP) ([10]) plutôt que le recours aux services de transport hybride CTAP.

(6) Afin que les États membres, les fournisseurs de certificats d'enregistrement de partie utilisatrice de portefeuille et les fournisseurs de portefeuille disposent de suffisamment de temps pour permettre aux unités de portefeuille d'authentifier et de valider les certificats d'enregistrement de partie utilisatrice de portefeuille, cette exigence ne devrait s'appliquer qu'à partir du 11 août 2028.

(7) Le règlement (UE) 2016/679 et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([11]) s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du présent règlement.

([7]) 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).

([8]) Règlement (UE) 2025/1208 du Conseil du 12 juin 2025 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation (JO L, 2025/1208, 20.6.2025, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres (JO L 385 du 29.12.2004, p. 1, ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) Proposition de norme de l'alliance Fido, Client to Authenticator Protocol (CTAP), 26 février 2026.

([11]) 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).

(8) 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 ([12]) et a rendu son avis le 17 avril 2026 ([13]).

(9) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Modification du règlement d'exécution (UE) 2024/2977

Le règlement d'exécution (UE) 2024/2977 est modifié comme suit:

1) L'article 3 *bis* suivant est inséré:

«*Article 3* bis

Protection du portrait

1. Outre les exigences en matière d'informations prévues par le règlement (UE) 2016/679, les fournisseurs de portefeuille veillent à ce que les solutions de portefeuille qu'ils fournissent adressent aux utilisateurs de portefeuille, lorsque les parties utilisatrices de portefeuille demandent la divulgation du portrait, un avertissement indiquant que la demande implique le partage de données biométriques et nécessite l'approbation de la divulgation sélective du portrait.

2. Pour la mise en œuvre de la divulgation sélective du portrait à une partie utilisatrice de portefeuille, les fournisseurs de portefeuille veillent à ce que les solutions de portefeuille demandent à l'utilisateur de portefeuille de confirmer explicitement et expressément la présentation du portrait.

3. Le portrait n'est pas conservé par les parties utilisatrices de portefeuille, à moins que son traitement ne soit nécessaire à des fins d'identification et d'authentification conformément au droit de l'Union en matière de protection des données ou lorsque cela est prévu par le droit de l'Union ou le droit national, conformément au droit de l'Union en matière de protection des données. Il n'est pas transféré à des pays tiers ou à des organisations internationales, à moins que le droit de l'Union en matière de protection des données ne l'autorise.».

2) À l'article 4, le paragraphe 1 est remplacé par le texte suivant:

«1. Les attestations électroniques d'attributs délivrées aux unités de portefeuille sont conformes à au moins une des normes figurant à l'annexe II du règlement d'exécution (UE) 2024/2979.».

3) À l'article 5, paragraphe 4, le point b) est remplacé par le texte suivant:

«b) lorsque l'attestation d'unité de portefeuille de l'unité de portefeuille à laquelle les données d'identification personnelle ont été délivrées a été révoquée;».

4) L'annexe est remplacée par le texte figurant à l'annexe I du présent règlement.

([12]) 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) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([13]) EDPS Formal comments on the draft Implementing Regulation as regards applicable standards and specifications and correcting Implementing Regulation (EU) 2024/2980 | Contrôleur européen de la protection des données.

Article 2

Modification du règlement d'exécution (UE) 2024/2979

Le règlement d'exécution (UE) 2024/2979 est modifié comme suit:

1) À l'article 3, le paragraphe 2 est supprimé.

2) À l'article 5, paragraphe 1, le point a) est remplacé par le texte suivant:

«a) n'effectuent d'opérations cryptographiques de portefeuille impliquant des actifs critiques stockés dans un dispositif cryptographique sécurisé de portefeuille et non requis pour l'authentification de l'utilisateur de portefeuille que dans les cas où lesdites applications ont authentifié avec succès les utilisateurs de portefeuille;».

3) L'article 5 *bis* suivant est inséré:

«*Article 5* bis

Mécanismes cryptographiques

Aux fins de l'article 4, paragraphe 2, les fournisseurs de portefeuille n'utilisent que les mécanismes cryptographiques visés à l'annexe I *bis*.».

4) L'article 6 est modifié comme suit:

a) le paragraphe 1 est remplacé par le texte suivant:

«1. Les fournisseurs de portefeuille délivrent des attestations d'unité de portefeuille pour chaque unité de portefeuille. Les fournisseurs de portefeuille apposent une signature ou un cachet sur les attestations d'unité de portefeuille de manière à ce que les signatures ou cachets puissent être validés au moyen d'un certificat énuméré conformément à la section 2, point 1), h), de l'annexe II du règlement d'exécution (UE) 2024/2980.»;

b) le paragraphe 2 est remplacé par le texte suivant:

«2. Les fournisseurs de portefeuille veillent à ce que les attestations d'unité de portefeuille visées au paragraphe 1 soient conformes aux spécifications techniques énoncées à l'annexe I *ter*.»;

c) au paragraphe 3, le point b) est remplacé par le texte suivant:

«b) fournissent aux utilisateurs de portefeuille des mécanismes sécurisés d'identification et d'authentification indépendants des unités de portefeuille;».

5) À l'article 9, paragraphe 2, le point b) est remplacé par le texte suivant:

«b) le nom, les coordonnées et l'identifiant unique de la partie utilisatrice de portefeuille correspondante ainsi que l'État membre dans lequel cette dernière est établie;».

6) À l'article 10, le paragraphe 1 est remplacé par le texte suivant:

«1. Les fournisseurs de portefeuille veillent à ce que les attestations électroniques d'attributs délivrées conformément aux spécifications techniques applicables aux politiques de divulgation intégrées communes au sens de l'annexe III puissent être traitées par les unités de portefeuille qu'ils fournissent.».

7) L'article 12 est modifié comme suit:

a) au paragraphe 2, le point c) est remplacé par le texte suivant:

«c) créer des signatures ou des cachets correspondant au moins au format obligatoire de signature ou de cachet visé à l'annexe IV;»;

b) le paragraphe 3 est remplacé par le texte suivant:

«3. Les applications de création de signature peuvent être intégrées aux instances de portefeuille ou extérieures à celles-ci.»;

c) le paragraphe suivant est inséré:

«4. Les applications de création de signature utilisées par les unités de portefeuille prennent en charge au moins l'interface de programmation d'applications visée à l'annexe IV.».

8) À l'article 14, le paragraphe 1 est supprimé.

9) L'article 14 *bis* suivant est inséré:

«*Article 14* bis

Label de confiance de l'UE pour le portefeuille d'identité numérique

1. Les fournisseurs de portefeuille veillent à ce que les unités de portefeuille affichent le label de confiance de l'UE pour le portefeuille d'identité numérique. Le label de confiance de l'UE pour le portefeuille d'identité numérique se présente sous la forme prévue aux annexes VI et VII.

2. Les fournisseurs de portefeuille font en sorte que les utilisateurs de portefeuille puissent accéder, via les unités de portefeuille, aux informations leur permettant de vérifier l'état de certification de la solution de portefeuille. À cette fin, les fournisseurs de portefeuille veillent à ce que, après l'enregistrement d'une solution de portefeuille, les unités de portefeuille correspondantes comprennent les URL fournies par la Commission européenne pour cette vérification. Les fournisseurs de portefeuille veillent à ce que leurs unités de portefeuille aient accès aux données du label de confiance de l'UE pour le portefeuille d'identité numérique qui sont conformes aux spécifications techniques énoncées à l'annexe VIII.

3. Les couleurs de référence du label de confiance de l'UE pour le portefeuille d'identité numérique sont les couleurs Pantone n° 661 et n° 116; ou, lorsque le procédé par quadrichromie est utilisé, le bleu (100 % cyan + 67 % magenta + 0 % jaune + 40 % noir) et le jaune (0 % cyan + 20 % magenta + 100 % jaune + 0 % noir); lorsque les couleurs RGB sont utilisées, les couleurs de référence sont le bleu (0 rouge + 51 vert + 153 bleu) et le jaune (255 rouge + 204 vert + 0 bleu).

4. La version en noir et blanc du label de confiance de l'UE pour le portefeuille d'identité numérique figurant à l'annexe VII peut être utilisée uniquement dans les cas où l'utilisation de la couleur n'est pas possible pour des raisons pratiques.

5. Lorsque le label de confiance de l'UE pour le portefeuille d'identité numérique est placé sur fond foncé, il peut être utilisé en négatif, en reprenant la même couleur de fond. Lorsque la version en couleurs du label de confiance de l'UE pour le portefeuille d'identité numérique est utilisée sur un fond coloré qui rend le label difficile à voir, une ligne de délimitation extérieure peut être tracée autour du label afin de renforcer le contraste avec le fond.

6. Le label de confiance de l'UE pour le portefeuille d'identité numérique a une taille minimale de 64 × 85 pixels à 150 dpi.

7. Les fournisseurs de portefeuille font en sorte que l'utilisation du label de confiance de l'UE pour le portefeuille d'identité numérique permette de déterminer clairement à quelle unité de portefeuille ce label se rapporte. Le label de confiance de l'UE pour le portefeuille d'identité numérique peut être associé à des éléments graphiques ou textuels indiquant clairement pour quelle unité de portefeuille il est utilisé, à condition qu'ils n'affectent ni sa capacité à être reconnu comme label de confiance de l'UE pour le portefeuille d'identité numérique, ni l'association à la liste des portefeuilles européens d'identité numérique certifiés visée à l'article 5 *quinquies* du règlement (UE) n° 910/2014.

8. Lorsque les fournisseurs de portefeuille ont révoqué une attestation d'unité de portefeuille, ils veillent à ce que le label de confiance de l'UE pour le portefeuille d'identité numérique ne soit plus affiché par l'unité de portefeuille correspondante.».

10) Les annexes I *bis* et I *ter* sont ajoutées, telles qu'elles figurent à l'annexe II et à l'annexe III du présent règlement.

11) L'annexe II est remplacée par l'annexe IV du présent règlement.

12) L'annexe III est remplacée par l'annexe V du présent règlement.

13) L'annexe IV est modifiée conformément à l'annexe VI du présent règlement.

14) L'annexe V est supprimée.

15) Le texte figurant à l'annexe VII du présent règlement est inséré comme annexe VI.

16) Le texte figurant à l'annexe VIII du présent règlement est inséré comme annexe VII.

17) Le texte figurant à l'annexe IX du présent règlement est inséré comme annexe VIII.

Article 3

Modifications du règlement d'exécution (UE) 2024/2980

Le règlement d'exécution (UE) 2024/2980 est modifié comme suit:

1. À l'article 5, le paragraphe 2 est remplacé par le texte suivant:

«2. Le cas échéant, la Commission établit, tient à jour et publie une liste reprenant les informations notifiées par les États membres concernant les fournisseurs de portefeuille, les fournisseurs de données d'identification personnelle, les fournisseurs de certificats d'accès de partie utilisatrice de portefeuille et les fournisseurs de certificats d'enregistrement de partie utilisatrice de portefeuille, telles qu'elles sont énumérées à l'annexe II, sections 2, 3, 4 et 5.».

2. L'annexe II du règlement d'exécution (UE) 2024/2980 est modifiée conformément à l'annexe X du présent règlement.

Article 4

Modifications du règlement d'exécution (UE) 2024/2982

Le règlement d'exécution (UE) 2024/2982 est modifié comme suit:

1) À l'article 1er, le paragraphe 2 est remplacé par le texte suivant:

«2) la présentation des attributs des données d'identification personnelle et des attestations électroniques d'attributs aux parties utilisatrices de portefeuille;».

2) L'article 3 est modifié comme suit:

a) le point 1) est remplacé par le texte suivant:

«1) authentifient et valident les certificats d'accès de partie utilisatrice de portefeuille lors d'interactions avec des parties utilisatrices de portefeuille sans déléguer l'exécution de ces processus à un navigateur du système d'exploitation ou à une autre application intermédiaire;»;

b) le point 2) est supprimé;

c) le point 3) est remplacé par le texte suivant:

«3) authentifient et valident les demandes introduites au moyen de certificats d'accès de partie utilisatrice de portefeuille;»;

d) le point 4) est remplacé par le texte suivant:

«4) authentifient et valident le certificat d'enregistrement de partie utilisatrice de portefeuille;»;

e) le point 5) est remplacé par le texte suivant:

«5) affichent aux utilisateurs de portefeuille les informations contenues dans les certificats d'accès de partie utilisatrice de portefeuille;»;

f) le point 8) est supprimé;

g) le point 9) est remplacé par le texte suivant:

«9) ne présentent aucun attribut demandé aux parties utilisatrices de portefeuille tant que les conditions suivantes ne sont pas remplies:

a) il a été vérifié que les politiques de divulgation intégrées ont été traitées au sein de l'unité de portefeuille conformément à l'article 10 du règlement d'exécution (UE) 2024/2979;

b) il a été vérifié que les utilisateurs de portefeuille ont approuvé partiellement ou intégralement la présentation;».

3) À l'article 4, le paragraphe 1 est remplacé par le texte suivant:

«1. Les fournisseurs de portefeuille veillent à ce que les solutions de portefeuille prennent en charge les protocoles et les interfaces figurant à l'annexe I pour la délivrance de données d'identification personnelle et d'attestations électroniques d'attributs aux unités de portefeuille.».

4) L'article 5 est modifié comme suit:

a) les paragraphes 1 et 2 sont remplacés par le texte suivant:

«1. Les fournisseurs de portefeuille veillent à ce que les solutions de portefeuille prennent en charge les protocoles et les interfaces permettant la présentation d'attributs aux parties utilisatrices de portefeuille, à distance et, le cas échéant, à proximité, conformément aux spécifications techniques figurant à l'annexe II.

2. Les fournisseurs de portefeuille veillent à ce que, à la demande des utilisateurs, les unités de portefeuille répondent aux demandes dûment authentifiées et validées des parties utilisatrices de portefeuille mentionnées à l'article 3, conformément aux spécifications techniques figurant à l'annexe II.»;

b) le paragraphe 5 est supprimé.

5) L'article 8 est remplacé par le texte suivant:

«*Article 8*

Entrée en vigueur

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

L'article 3, paragraphe 4, s'applique à compter du 11 août 2028.

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

6) L'annexe est supprimée.

7) Le texte figurant à l'annexe XI du présent règlement est ajouté en tant qu'annexe I.

8) Le texte figurant à l'annexe XII du présent règlement est ajouté en tant qu'annexe II.

Article 5

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 15 juillet 2026.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE I

«ANNEXE

Spécifications techniques relatives aux données d'identification personnelle visées à l'article 3, paragraphe 3

Section 1: Ensemble de données d'identification des personnes physiques

Tableau 1

Données d'identification personnelle obligatoires pour les personnes physiques soumises à la divulgation sélective

Identifiant de données	Définition
`family_name`	Nom(s) de famille actuel(s) de l'utilisateur auquel se rapportent les données d'identification personnelle.
`given_name`	Prénom(s) actuel(s), y compris, le cas échéant, le(s) deuxième(s) prénom(s), de l'utilisateur auquel se rapportent les données d'identification personnelle.
`birth_date`	Jour, mois et année de naissance de l'utilisateur auquel se rapportent les données d'identification personnelle.
`birth_place`	Le code pays alpha-2, tel que spécifié dans la norme ISO 3166-1, ou la subdivision de l'État, la province, le district, le territoire ou la municipalité, la ville ou le village où est né l'utilisateur auquel les données d'identification personnelle se rapportent.
`nationality`	Un ou plusieurs codes pays alpha-2 spécifiés dans la norme ISO 3166-1, représentant la nationalité de l'utilisateur auquel se rapportent les données d'identification personnelle.
`portrait`	Sauf refus exprès de l'utilisateur, le cas échéant, l'image faciale de l'utilisateur auquel se rapportent les données d'identification personnelle, conforme aux exigences de qualité applicables à un type d'image frontale complète du visage énoncées dans la norme ISO/IEC 39794-5 ou, aux fins de la compatibilité rétrospective, dans la norme ISO/IEC 19794-5, paragraphes 8.2, 8.3 et 8.4, fournie sous forme de données d'image encodées sans les en-têtes ou les blocs comme spécifié dans le paragraphe 5 de la norme ISO/IEC 19794-5, à l'exception des données d'image proprement dites (un JPEG), est applicable à partir du 11 août 2028.

— Les États membres peuvent prévoir que l'utilisateur a la faculté de refuser l'insertion du portrait dans les données d'identification personnelle.

— Les États membres doivent veiller à ce que la divulgation sélective s'applique à chaque identifiant de données, y compris le portrait.

— Si la date de naissance de la personne physique n'est pas connue, les États membres doivent choisir des valeurs appropriées conformes aux spécifications mentionnées aux sections 4.1 ou 4.2 (selon le cas) de la présente annexe.

— Si la nationalité de la personne physique est inconnue, les États membres doivent utiliser la valeur 'QU'.

— Si la personne physique ne possède pas de nationalité, les États membres doivent utiliser la valeur 'QS'.

— Si l'utilisateur refuse l'insertion du portrait, les États membres doivent laisser la valeur vide.

Tableau 2

Données d'identification personnelle facultatives pour les personnes physiques soumises à la divulgation sélective

Identifiant de données	Définition
`resident_address`	L'adresse complète du lieu où l'utilisateur auquel se rapportent les données d'identification personnelle réside actuellement ou peut être contacté (nom de rue, numéro de maison, ville, etc.).
`resident_country`	Le pays où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle, sous la forme d'un code pays alpha-2, tel que spécifié dans la norme ISO 3166-1.
`resident_state`	La subdivision de l'État, la province, le district ou le territoire où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle.
`resident_city`	La municipalité, la ville ou le village où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle.
`resident_postal_code`	Le code postal du lieu où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle.
`resident_street`	Le nom de la rue où réside actuellement l'utilisateur auquel se rapportent les données d'identification personnelle, y compris le numéro de la maison et tout affixe ou suffixe de ce numéro.
`personal_administrative_number`	Une valeur attribuée à l'utilisateur auquel se rapportent les données d'identification personnelle, qui est unique parmi tous les numéros administratifs personnels délivrés par le fournisseur de données d'identification personnelle. Lorsque les États membres choisissent d'inclure cet attribut, ils doivent décrire dans leurs schémas d'identification électronique en vertu desquels les données d'identification personnelle sont délivrées la politique qu'ils appliquent aux valeurs de cet attribut, y compris, le cas échéant, les conditions spécifiques applicables au traitement de cette valeur.
`family_name_birth`	Nom(s) de famille de l'utilisateur auquel se rapportent les données d'identification personnelle au moment de la naissance.
`given_name_birth`	Prénom(s), y compris le(s) deuxième(s) prénom(s), de l'utilisateur auquel se rapportent les données d'identification personnelle au moment de la naissance.
`sex`	La valeur est l'une des suivantes: 0 = inconnu; 1 = masculin; 2 = féminin; 3 = autre; 4 = inter; 5 = divers; 6 = ouvert; 9 = sans objet. Pour les valeurs 0, 1, 2 et 9, la norme ISO/IEC 5218 s'applique.
`email_address`	Adresse de courrier électronique de l'utilisateur auquel se rapportent les données d'identification personnelle [conformément à la norme RFC 5322 [1]].

Identifiant de données	Définition
`mobile_phone_number`	Numéro de téléphone portable de l'utilisateur auquel se rapportent les données d'identification personnelle, commençant par le symbole "+", comme préfixe d'appel international, et l'indicatif téléphonique international, suivis de numéros uniquement.

([1]) P. Resnick, éd., "Format de message Internet", RFC 5322, octobre 2008.

Section 2: Ensemble de donnés d'identification des personnes morales

Tableau 3

Données d'identification personnelle obligatoires pour les personnes morales

Identifiant de données
Dénomination sociale actuelle
Un identifiant unique créé par l'État membre expéditeur conformément aux spécifications techniques aux fins de l'identification transfrontière et qui soit aussi persistant que possible dans le temps

— Lorsqu'un identifiant de données n'est pas connu pour la personne ou ne peut pas être délivré autrement dans le cadre de l'ensemble de données d'identification personnelle, les États membres doivent utiliser à la place une valeur d'attribut adaptée à la situation.

Tableau 4

Données d'identification personnelle facultatives pour les personnes morales

Identifiant de données
Adresse actuelle
Numéro d'identification TVA
Numéro de référence fiscal
Identifiant unique européen visé dans la directive (UE) 2017/1132 du Parlement européen et du Conseil ([1])
Identifiant d'entité juridique (LEI) visé dans le règlement d'exécution (UE) 2022/1860 de la Commission ([2])
Numéro d'enregistrement et d'identification des opérateurs économiques (numéro EORI) visé dans le règlement d'exécution (UE) n° 1352/2013 de la Commission ([3])
Numéro d'accise visé à l'article 2, point 12), du règlement (UE) n° 389/2012 du Conseil ([4])

([1]) Directive (UE) 2017/1132 du Parlement européen et du Conseil du 14 juin 2017 relative à certains aspects du droit des sociétés (JO L 169 du 30.6.2017, p. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) Règlement d'exécution (UE) 2022/1860 de la Commission du 10 juin 2022 définissant des normes techniques d'exécution pour l'application du règlement (UE) n° 648/2012 du Parlement européen et du Conseil en ce qui concerne les normes, les formats, la fréquence et les méthodes et modalités de déclaration (JO L 262 du 7.10.2022, p. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Règlement d'exécution (UE) n° 1352/2013 de la Commission du 4 décembre 2013 établissant les formulaires prévus par le règlement (UE) n° 608/2013 du Parlement européen et du Conseil concernant le contrôle, par les autorités douanières, du respect des droits de propriété intellectuelle (JO L 341 du 18.12.2013, p. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) Règlement (UE) n° 389/2012 du Conseil du 2 mai 2012 concernant la coopération administrative dans le domaine des droits d'accise et abrogeant le règlement (CE) n° 2073/2004 (JO L 121 du 8.5.2012, p. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

3. Section 3: Ensemble de métadonnées relatives aux données d'identification des personnes

Tableau 5

Métadonnées relatives aux données d'identification des personnes

Identifiant de données	Définition	Présence
`issuing_authority`	Nom de l'autorité administrative qui a délivré les données d'identification personnelle, ou code pays ISO 3166 alpha-2 de l'État membre concerné s'il n'existe pas d'autorité distincte habilitée à délivrer les données d'identification personnelle.	Obligatoire
`issuing_country`	Code pays alpha-2, tel que spécifié dans la norme ISO 3166-1, du pays ou territoire du fournisseur des données d'identification personnelle.	Obligatoire
`expiry_date`	Date (et, si possible, heure) à laquelle la période de validité administrative des données d'identification personnelle expire.	Facultatif
`document_number`	Un numéro pour les données d'identification personnelle, attribué par le fournisseur de données d'identification personnelle.	Facultatif
`issuing_jurisdiction`	Code de subdivision du pays correspondant à l'entité territoriale qui a émis les données d'identification personnelle, conformément au paragraphe 8 de la norme ISO 3166-2:2020. La première partie du code est identique à la valeur correspondant au pays de délivrance.	Facultatif
`issuance_date`	Date et, si possible, heure auxquelles la période de validité administrative des données d'identification personnelle a commencé.	Facultatif

4) Section 4: Encodage des attributs de données d'identification des personnes physiques

— Les données d'identification des personnes physiques doivent être délivrées conformément aux normes mentionnées à l'annexe II du règlement d'exécution (UE) 2024/2979, paragraphes 5 (format SD-JWT VC) et 6 (format ISO/IEC-mdoc), applicables aux attestations électroniques d'attributs. Les paragraphes 5.2.2, 5.2.4, 5.2.5, EAA-6.1-03, 6.2.2, 6.2.3, 6.2.4 et 6.2.5 ne s'appliquent pas.

— L'encodage des données d'identification des personnes physiques doit être conforme aux spécifications techniques énoncées aux sections 4.1 et 4.2 de la présente annexe.

4.1 Encodage des données d'identification des personnes physiques au format ISO/IEC-mdoc

— Le type d'attestation pour les données d'identification personnelle au format ISO/IEC-mdoc doit être 'eu.europa.ec.eudi.pid.1'. L'identifiant de l'espace de noms pour les attributs de données d'identification personnelle figurant dans la présente annexe doit être 'eu.europa.ec.eudi.pid.1'.

— Si les données d'identification personnelle comprennent des données pour lesquelles la présente annexe ne prévoit pas d'identifiants de données, ces données doivent être définies dans un espace de noms (infra)national alloué aux données d'identification personnelle qui utilise le format général eu.europa.ec.eudi.pid.[code pays ISO 3166-1 alpha-2 ou code région ISO 3166-2] suivi d'un point et d'un numéro de version facultatifs.

— Si l'espace de noms (infra)national est utilisé, son programme, comprenant tous les identifiants de données, leur définition, leur présence et leur format d'encodage, doit être publié conformément à l'article 8 du règlement d'exécution (UE) 2025/1569 de la Commission ([1]).

— Les données d'identification personnelle et leurs métadonnées mentionnées aux sections 1 et 3 de la présente annexe doivent figurer dans les éléments de données d'identification personnelle au sens des spécifications du format ISO/IEC-mdoc.

— Le membre deviceKey au sein du membre deviceKeyInfo de l'instance du type MobileSecurityObject contient une clé publique.

— Cette clé publique doit correspondre à une clé privée qui est stockée dans le dispositif cryptographique sécurisé de portefeuille ("wallet secure cryptographic device", ou "WSCD") de l'utilisateur de portefeuille.

— L'en-tête protégé de la signature numérique CB-AdES qui signe une donnée d'identification personnelle au format ISO/IEC-mdoc doit contenir les paramètres d'en-tête x5u et x5t, tous deux spécifiés dans la RFC 9360 ([2]).

— L'algorithme de hachage utilisé dans le paramètre d'en-tête x5t doit être SHA-256.

— Les exigences applicables à l'encodage des données d'identification personnelle au format ISO/IEC-mdoc figurent dans le tableau 6.

Tableau 6

Exigences applicables à l'encodage des données d'identification personnelle au format ISO/IEC-mdoc

Identifiant de données	Identifiant d'attribut	Format d'encodage
family_name	family_name	tstr
given_name	given_name	tstr
birth_date	birth_date	full-date
birth_place	place_of_birth	place_of_birth
nationality	nationality	nationalities
resident_address	resident_address	tstr
resident_country	resident_country	tstr
resident_state	resident_state	tstr
resident_city	resident_city	tstr
resident_postal_code	resident_postal_code	tstr
resident_street	resident_street	tstr
personal_administrative_number	personal_administrative_number	tstr
portrait	portrait	bstr
family_name_birth	family_name_birth	tstr
given_name_birth	given_name_birth	tstr
sex	sex	uint

([1]) Règlement d'exécution (UE) 2025/1569 de la Commission du 29 juillet 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les attestations électroniques d'attributs qualifiées et les attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte (JO L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([2]) J. Schaad, "Signature et chiffrement d'objet CBOR (COSE): paramètres d'en-tête pour porter et référencer les certificats X.509" (https://datatracker.ietf.org/doc/rfc9360/).

Identifiant de données	Identifiant d'attribut	Format d'encodage
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate ou full-date
issuing_authority	issuing_authority	tstr
issuing_country	issuing_country	tstr
document_number	document_number	tstr
issuing_jurisdiction	issuing_jurisdiction	tstr
issuance_date	issuance_date	tdate ou full-date

— La notation du format d'encodage des attributs spécifiés dans le tableau 6 utilise les types de représentation spécifiés dans la RFC 8610 ([3]), moyennant les exigences supplémentaires suivantes:

a) les tstr doivent être encodées en UTF-8;

b) les tstr doivent prendre en charge toute la plage Unicode;

c) les tstr doivent avoir une longueur maximale de 150 caractères;

d) les dates doivent être encodées conformément à la RFC 8943 ([4]);

e) l'attribut full-date doit être interprété comme #6.1004(tstr), le tag 1004 étant spécifié dans la RFC 8943;

f) l'attribut tdate doit contenir une chaîne date-heure telle que spécifiée dans la RFC 3339 ([5]);

g) l'attribut full-date doit contenir une chaîne full-date telle que spécifiée dans la RFC 3339, conformément à la RFC 8943;

h) sauf indication contraire, la représentation d'une date dans les attributs:

— ne doit pas utiliser de fractions de seconde;

— ne doit pas utiliser de décalage de temps local par rapport à l'UTC et le décalage de temps spécifié dans la RFC 3339 doit être fixé à 'Z';

i) les nombres entiers ayant les types majeurs 0 et 1 doivent être aussi petits que possible, comme spécifié dans la RFC 8949, section 4.2 ([6]);

j) l'attribut place_of_birth doit contenir au moins une des paires clé-valeur suivantes: 'country', 'region' ou 'locality';

k) l'expression de la longueur dans une bstr, une tstr, un tableau ou une table associative doit être aussi courte que possible, comme spécifié dans la RFC 8949, section 4.2;

([3]) C. Vigano et H. Birkholz, "Langage de définition concise de données (CDDL): convention de notation pour exprimer la représentation concise d'objet binaire CBOR) et les structures de données Jason", RFC 8610, juin 2019.
([4]) M. Jones, A. Nadalin et J. Richter, "Étiquettes de représentation concise d'objet binaire (CBOR) pour la date", RFC 8943, novembre 2020.
([5]) G. Klyne et C. Newman, "La date et l'heure sur l'Internet: horodatages", RFC 3339, juillet 2002.
([6]) C. Bormann et P. Hoffman, "Représentation concise d'objet binaire (CBOR)", RFC 8949, décembre 2020.

l) l'attribut nationality doit être encodé sous la forme d'un tableau de codes pays alpha-2, conformément à la norme ISO 3166-1. Lorsque la notation CDDL telle que spécifiée dans le RFC 8610 est utilisée, l'encodage de cet attribut doit être le suivant:

— nationalities = [+ CountryCode];

— CountryCode = tstr; code pays alpha-2 spécifié dans la norme ISO 3166-1;

— lorsqu'un utilisateur de portefeuille auquel se rapportent les données d'identification personnelle possède plusieurs nationalités et que le fournisseur de données d'identification personnelle atteste ces nationalités multiples, le fournisseur de données d'identification personnelle peut inclure toutes les nationalités dans les données d'identification personnelle;

— l'attribut place_of_birth doit être encodé comme un type place_of_birth. Lorsque la notation CDDL telle que spécifiée dans le RFC 8610 est utilisée, l'encodage de cet attribut doit être le suivant:

place_of_birth =

{

? 'country': tstr; un code pays alpha-2 unique comme spécifié dans la norme ISO 3166-1

? 'region': tstr; le nom de la subdivision de l'État, de la province, du district ou du territoire

? 'locality': tstr; le nom de la municipalité, de la ville ou du village

}

4.2 Exigences applicables à l'encodage des données d'identification personnelle au format SD-JWT VC

— Les données d'identification personnelle et leurs métadonnées mentionnées dans la présente section doivent figurer dans les données d'identification personnelle en tant que revendications au sens des spécifications du format SD-JWT VC.

— Toutes les revendications figurant dans les données d'identification personnelle délivrées, mentionnées au tiret précédent, doivent pouvoir faire l'objet d'une divulgation sélective de manière individuelle, à l'exception des revendications définies comme ne pouvant pas faire l'objet d'une divulgation sélective dans le format SD-JWT VC.

— Le tableau 7 détermine l'encodage des noms de revendications qui sont des noms publics.

— Le tableau 8 détermine l'encodage des noms de revendications qui sont propres aux données d'identification personnelle.

— Les chaînes JSON utilisées dans des données d'identification personnelle encodées au format SD-JWT VC doivent être encodées en UTF-8 et prendre en charge toute la plage Unicode, sauf indication contraire expresse dans le tableau 8 ci-dessous ou dans les références qui y figurent.

— Les revendications JWT nbf et exp, telles que définies dans la RFC 7519 ([7]), doivent être utilisées pour exprimer la période de validité technique des données d'identification personnelle en conformité avec le format SD-JWT VC.

([7]) J. Jones et autres, "Jeton JSON sur la Toile (JWT)", RFC 7519, mai 2015.

— Les données d'identification personnelle doivent comprendre la revendication cnf telle que définie dans la RFC 7800 ([8]), qui doit être une clé publique générée à partir d'une clé privée stockée dans le WSCD de l'unité de portefeuille de l'utilisateur de portefeuille.

— L'en-tête protégé de la signature numérique qui signe une donnée d'identification personnelle au format SD-JWT VC contient les paramètres d'en-tête x5u et x5t#S256, spécifiés dans la RFC 7515 ([9]).

Tableau 7

Exigences applicables à l'encodage des données d'identification personnelle au format SD-JWT VC utilisant des noms publics

Identifiant de données	Identifiant d'attribut	Format d'encodage
`family_name`	`family_name`	chaîne de caractères
`given_name`	`given_name`	chaîne de caractères
`birth_date`	`birthdate`	chaîne de caractères, ISO 8601-1, format AAAA-MM-JJ
`birth_place`	`place_of_birth`	structure JSON
`nationality`	`nationalities`	tableau de chaînes
`resident_address`	`address.formatted`	chaîne de caractères
`resident_country`	`address.country`	chaîne de caractères
`resident_state`	`address.region`	chaîne de caractères
`resident_city`	`address.locality`	chaîne de caractères
`resident_postal_code`	`address.postal_code`	chaîne de caractères
`resident_street`	`address.street_address`	chaîne de caractères
`family_name_birth`	`birth_family_name`	chaîne de caractères
`given_name_birth`	`birth_given_name`	chaîne de caractères
`email_address`	`email`	chaîne de caractères
`mobile_phone_number`	`phone_number`	chaîne de caractères
`portrait`	`picture`	chaîne de caractères; URL de données contenant un portrait encodé en base 64 au format JPEG

([8]) M. Jones et autres, "Sémantique de clé de preuve de possession pour jetons JSON de la Toile", RFC 7800, avril 2016.
([9]) M. Jones et autres, "Signature JSON sur la Toile (JWS)", RFC 7515, mai 2015.

Tableau 8

Exigences applicables à l'encodage des données d'identification personnelle au format SD-JWT VC utilisant des noms privés

Identifiant de données	Identifiant d'attribut	Format d'encodage
`expiry_date`	`date_of_expiry`	chaîne de caractères, ISO 8601-1, format AAAA-MM-JJ
`issuance_date`	`date_of_issuance`	chaîne de caractères, ISO 8601-1, format AAAA-MM-JJ
`personal_administrative_number`	`personal_administrative_number`	chaîne de caractères
`sex`	`sex`	valeur numérique
`issuing_authority`	`issuing_authority`	chaîne de caractères
`issuing_country`	`issuing_country`	chaîne de caractères
`document_number`	`document_number`	chaîne de caractères
`issuing_jurisdiction`	`issuing_jurisdiction`	chaîne de caractères

— Le type de base des données d'identification personnelle doit être 'urn:eudi:pid:1', inclus dans la revendication vct. Toutes les données d'identification personnelle doivent utiliser des types compris dans l'espace de noms 'urn:eudi:pid:'.

— Si les données d'identification personnelle comprennent des attributs qui ne sont pas spécifiés dans la présente annexe, ces attributs sont définis au sein d'un type (infra)national.

— Si le type (infra)national est utilisé, son programme, comprenant tous les identifiants de données, leur définition, leur présence et leur format d'encodage, doit être défini dans un programme publié conformément à l'article 8 du règlement d'exécution (UE) 2025/1569.

Section 5: Détails de l'infrastructure de confiance

La liste des fournisseurs de données d'identification personnelle mise à disposition par la Commission conformément au règlement d'exécution (UE) 2024/2980 permet d'authentifier les données d'identification personnelle.».

ANNEXE II

«*ANNEXE I bis*

Mécanismes cryptographiques visés à l'article 5 *bis*

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]).».

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

ANNEXE III

«ANNEXE I ter

Spécifications techniques pour les attestations d'unité de portefeuille visées à l'article 6, paragraphe 2 *bis*

1) Une attestation d'unité de portefeuille doit comprendre une ou plusieurs attestations d'instance de portefeuille et une ou plusieurs attestations de clé.

2) L'attestation d'instance de portefeuille et les attestations de clé doivent satisfaire aux exigences suivantes:

a) Exigences en matière de format

— FR-WIA-1: une attestation d'instance de portefeuille doit être un jeton Web JSON (JWT) tel que défini dans la RFC 7519 ([1]), sur lequel le fournisseur de portefeuille a apposé sa signature ou son cachet au moyen d'une signature JAdES compacte conforme au niveau de base B.

— FR-WIA-1.1: une attestation d'instance de portefeuille doit être une attestation de portefeuille telle que définie à l'appendice E de la spécification "OpenID for Verifiable Credential Issuance v1.0" ([2]) ('OID4VCI ') et étendue comme indiqué dans les paragraphes C-WIA-1 et C-WIA-2 ci-dessous.

— FR-KA-1: une attestation de clé doit être un JWT tel que défini dans la RFC 7519, sur lequel le fournisseur de portefeuille a apposé sa signature ou son cachet au moyen d'une signature JAdES compacte conforme au niveau de base B.

— FR_KA_1.1: une attestation de clé doit être une attestation de clé telle que définie à l'appendice D de la spécification OID4VCI, étendue comme indiqué dans les paragraphes C_KA-1 et C_KA-2 ci-dessous.

b) Exigences en matière de transport

— TR-WIA-1: une unité de portefeuille doit utiliser une attestation d'instance de portefeuille lors de la délivrance de données d'identification personnelle, d'attestations électroniques d'attributs qualifiées ou non qualifiées ou d'attestations électroniques d'attributs fournies par un organisme du secteur public responsable d'une source authentique ou pour son compte.

— TR-WIA-2: un fournisseur de portefeuille doit vérifier l'intégrité de l'instance de portefeuille et apposer sa signature ou son cachet sur l'attestation d'instance de portefeuille.

— TR-WIA-2.1: lorsqu'un fournisseur de portefeuille délivre une attestation d'instance de portefeuille, la différence entre l'heure à laquelle le fournisseur de portefeuille a vérifié l'intégrité de l'instance de portefeuille et l'heure qu'il indiquera dans le paramètre d'en-tête 'exp' de l'attestation d'instance de portefeuille délivrée doit être inférieure à 24 heures.

— TR-WIA-2.2: le fournisseur de portefeuille doit veiller à ce qu'une unité de portefeuille contienne les attestations d'instance de portefeuille nécessaires à la délivrance des données d'identification personnelle et des attestations électroniques d'attributs.

— TR-WIA-3: lors de la délivrance, une unité de portefeuille doit envoyer une attestation d'instance de portefeuille au serveur d'autorisation dans la demande d'autorisation poussée et la demande de jeton, comme indiqué dans la spécification OID4VCI.

— TR-WIA-3.1: une unité de portefeuille doit envoyer l'attestation d'instance de portefeuille accompagnée d'une preuve de possession ('PoP'), comme indiqué à l'appendice E de la spécification OID4VCI.

— TR-WIA-3.2: une unité de portefeuille ne doit envoyer la même attestation d'instance de portefeuille qu'à un seul serveur d'autorisation.

([1]) RFC 7519: Jeton JSON sur la Toile (JWT), mai 2015.
([2]) "OpenID for Verifiable Credential Issuance v1.0", https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

— TR-WIA-3.2.1: lorsqu'un fournisseur de portefeuille utilise l'option 'per-issuer reuse' spécifiée dans le paragraphe R_WIA_1 ci-dessous, une unité de portefeuille peut envoyer plusieurs fois une attestation d'instance de portefeuille au même serveur d'autorisation.

— TR-WIA-3.2.2: lorsqu'un fournisseur de portefeuille n'utilise pas l'option 'per-issuer reuse', une unité de portefeuille doit utiliser une attestation d'instance de portefeuille dans un seul processus de délivrance au maximum.

— TR-WIA-4: lorsqu'un serveur d'autorisation reçoit une attestation d'instance de portefeuille, il doit vérifier la signature de l'attestation d'instance de portefeuille en utilisant la clé publique contenue dans le certificat de signature inclus dans le paramètre 'x5c' de l'en-tête JOSE de l'attestation d'instance de portefeuille.

— TR-WIA-4.1: le serveur d'autorisation doit vérifier également que ce certificat de signature peut être vérifié avec une ancre de confiance sur la liste des fournisseurs de portefeuille visée à l'article 5 du règlement d'exécution (UE) 2024/2980, en utilisant éventuellement des certificats intermédiaires inclus dans le paramètre x5c.

— TR-WIA-4.2: le serveur d'autorisation doit vérifier que l'attestation d'instance de portefeuille n'a pas expiré.

— TR-WIA-4.3: le serveur d'autorisation doit vérifier la signature de la PoP en utilisant la clé publique figurant dans la revendication 'cnf'.

— TR_KA-1: une unité de portefeuille doit utiliser une attestation de clé lors de la délivrance de données d'identification personnelle et lors de la délivrance d'attestations électroniques d'attributs qualifiées ou non qualifiées liées à un appareil ou d'attestations électroniques d'attributs fournies par un organisme du secteur public responsable d'une source authentique ou pour son compte.

— TR_KA-1.1: une unité de portefeuille ne doit pas utiliser d'attestation de clé lors de la délivrance d'attestations électroniques d'attributs qualifiées ou non qualifiées liées à un appareil ou d'attestations électroniques d'attributs fournies par un organisme du secteur public responsable d'une source authentique ou pour son compte.

— TR_KA-2: un fournisseur de portefeuille doit fournir à une unité de portefeuille des attestations de clé différentes pour le WSCD de l'unité de portefeuille et pour chacun de ses magasins de clés.

— TR_KA-2.1: le fournisseur de portefeuille doit apposer sa signature ou son cachet sur une attestation de clé après avoir vérifié que les clés attestées dans l'attestation de clé sont stockées dans le WSCD de l'unité de portefeuille ou le magasin de clés décrit dans l'attestation de clé.

— TR_KA-2.2: une attestation de clé doit contenir au moins une clé publique attestée. Le nombre de clés contenues dans l'attestation de clé envoyée à un émetteur de justificatifs d'identité ne devrait pas dépasser la taille de lot maximale définie par ledit émetteur dans ses métadonnées; voir ETSI TS 119 472-3 ([3]), paramètre 'credential_configurations_supported. credential_metadata.credential_reuse_policy.options.batch_size'.

— TR_KA-2.3: un fournisseur de portefeuille doit inclure une clé publique (correspondant à une clé privée stockée dans le WSCD ou le magasin de clés de l'unité de portefeuille) dans une seule attestation de clé au maximum.

— TR_KA-2.4: une unité de portefeuille doit utiliser une attestation de clé lors d'un seul processus de délivrance ou de redélivrance de justificatif d'identité au maximum.

— TR_KA-2.5: un fournisseur de portefeuille doit veiller à ce qu'une unité de portefeuille soit en possession des attestations de clé nécessaires à la délivrance des données d'identification personnelle et des attestations électroniques d'attributs liées à un appareil.

([3]) ETSI, "Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 3: JAdES levels and baseline profiles", ETSI TS 119 472-3, V1.1.1, mars 2026.

— TR_KA-3: en cas de nécessité lors de la délivrance, une unité de portefeuille doit contenir une attestation de clé dans le champ 'proofs' d'une demande de justificatif d'identité adressée à l'émetteur de justificatifs d'identité, comme indiqué dans la spécification OID4VCI, dans une preuve de type 'jwt' ou de type 'attestation'.

— TR_KA_3.1: lorsqu'une unité de portefeuille comprend une attestation de clé dans un élément 'jwt', elle doit apposer une signature ou un cachet sur l'attestation de clé en utilisant la clé privée correspondant à la clé publique située à l'index 0 du tableau 'attested_keys' dans l'objet 'key_attestation'.

— TR_KA-4: lorsqu'un émetteur de justificatifs d'identité émet des justificatifs liés à un appareil, il doit indiquer dans le paramètre 'proof_types_supported' de ses métadonnées, comme spécifié à la section 12.2.4 de la spécification OID4VCI, qu'il prend en charge à la fois le type de preuve 'jwt' et le type de preuve 'attestation' pour les attestations de clé qui contiennent l'objet 'key_attestations_required'.

— TR_KA-4.1: lorsqu'un émetteur de justificatifs d'identité délivre des justificatifs non liés à un appareil, il doit omettre les paramètres 'proof_types_supported' et 'cryptographic_binding_methods_supported' dans ses métadonnées d'émetteur de justificatifs d'identité.

— TR_KA-5: lorsqu'un émetteur de justificatifs d'identité reçoit une attestation de clé dans un type de preuve 'jwt' ou 'attestation', il doit vérifier la signature de l'attestation de clé en utilisant la clé publique contenue dans le certificat de signature inclus dans le paramètre 'x5c' de l'en-tête JOSE de l'attestation de clé et s'assurer que ce certificat de signature est relié à une ancre de confiance figurant sur la liste des fournisseurs de portefeuille visée à l'article 5 du règlement d'exécution (UE) 2024/2980, en utilisant éventuellement des certificats intermédiaires inclus dans le paramètre 'x5c'.

— TR_KA-6: lorsqu'un émetteur de justificatifs d'identité reçoit une attestation de clé dans un type de preuve 'jwt', il doit vérifier la signature de l'élément 'jwt' en utilisant la clé située à l'index 0 du tableau 'attested_keys' dans l'objet 'key_attestation' inclus dans l'élément 'jwt'.

— TR_KA-6.1: l'émetteur de justificatifs d'identité doit vérifier que le champ 'nonce' de l'élément 'jwt' comprend un c_nonce valide obtenu depuis son nonce_endpoint, comme indiqué dans la spécification OID4VCI.

— TR_KA-7: lorsqu'un émetteur de justificatifs d'identité reçoit une attestation de clé dans un type de preuve 'attestation', il doit vérifier que l'objet 'key_attestation' contient un c_nonce valide obtenu depuis son nonce_endpoint.

— TR_KA-8: un fournisseur de données d'identification personnelle doit veiller à ce que les données d'identification personnelle soient reliées à une clé publique provenant d'une attestation de clé mentionnant un WSCD.

c) Exigences en matière de contenu

— C_WIA-1: une attestation d'instance de portefeuille doit comprendre les éléments suivants:

— la revendication 'wallet_name' définie à l'appendice E de la spécification OID4VCI, dont la valeur doit être l'identifiant de la solution de portefeuille qui figure sur la liste des fournisseurs de portefeuille visée à l'article 5 du règlement d'exécution (UE) 2024/2980;

— une revendication 'wallet_version' ([4]), qui doit être une chaîne de caractères dont la valeur doit être la version de la solution de portefeuille;

— une revendication 'wallet_solution_certification_information', qui doit être un objet JSON contenant des informations sur l'organisme d'évaluation de la conformité qui a certifié la solution de portefeuille, le numéro de certification, le cas échéant, et d'autres informations pertinentes concernant la certification;

([4]) Cette revendication est définie dans le présent règlement d'exécution de la Commission car elle ne fait partie de la spécification OID4VCI.

— une revendication 'client_status', contenant deux sous-champs:

— 'status': une référence à la liste d'états telle que définie à l'appendice E de la spécification OID4VCI, qui représente l'état de révocation de l'instance de portefeuille. Voir la section e) ci-dessous pour plus de détails;

— 'exp': une NumericDate, telle que spécifiée dans la RFC 7519, indiquant jusqu'à quel moment le fournisseur de portefeuille maintiendra l'état de révocation à l'index de la liste d'états référencé dans le champ 'status';

— la revendication 'exp' définie à l'appendice E de la spécification OID4VCI.

— *REMARQUE:* la revendication 'client_status.status' dans une attestation d'instance de portefeuille représente l'état de révocation de l'instance de portefeuille, et non l'état de révocation de l'attestation elle-même. Comme décrit dans le paragraphe R_WIA-1 ci-dessous, un fournisseur de portefeuille peut décider de limiter la portée de chaque attestation d'instance de portefeuille à un serveur d'autorisation spécifique en se fondant sur le fait que toutes les attestations envoyées à ce serveur contiennent la même valeur d'index dans l'entrée 'client_status.status'.

— *REMARQUE:* la valeur 'idx' dans la revendication 'status' peut être utilisée comme identifiant unique (pairwise) de l'instance de portefeuille et de l'unité de portefeuille.

— C_WIA-2: une attestation d'instance de portefeuille devrait comprendre également la revendication 'wallet_link' définie à l'appendice E de la spécification OID4VCI, la valeur de cette revendication étant un URI permettant d'obtenir des informations supplémentaires sur la solution de portefeuille.

— C_WIA-3: un serveur d'autorisation ne doit pas interpréter le paramètre 'exp' au niveau le plus élevé d'une attestation d'instance de portefeuille comme étant la fin de la période de maintien de la révocation de l'instance de portefeuille.

— *REMARQUE:* le paramètre 'exp' au niveau le plus élevé d'une attestation d'instance de portefeuille indique à quel moment l'attestation proprement dite expire.

— C_KA-1: une attestation de clé comprend:

— les revendications 'key_storage' et 'user_authentification' définies à l'appendice D de la spécification OID4VCI.

— Les attributs 'key_storage' et 'user_authentification' doivent avoir la valeur 'iso_18045_high' lorsqu'une attestation de clé mentionne un WSCD;

— la revendication "certification" définie à l'appendice D de la spécification OID4VCI, contenant une URL permettant d'obtenir des informations sur la certification obtenue par le WSCD ou le magasin de clés, à titre indicatif le schéma tel que Common Criteria ou GlobalPlatform, les exigences évaluées telles que le profil de protection applicable et le niveau d'évaluation.

— Ces informations permettent de déterminer si le stockage de la clé est un WSCD;

— une revendication 'key_storage_status', contenant deux sous-champs:

— 'status': une référence à la liste d'états telle que définie à l'appendice D.1 de la spécification OID4VCI. La valeur représente soit l'état de révocation du WSCD ou du type de magasin de clés utilisé pour stocker les clés attestées, soit, dans le cadre de l'option d'index per-key-attestation, l'état de révocation du WSCD ou du magasin de clés d'une unité de portefeuille individuelle. Voir R_KA_1 ci-dessous pour les options d'attribution d'index disponibles;

— 'exp': une NumericDate, telle que spécifiée dans la RFC 7519, indiquant jusqu'à quel moment le fournisseur de portefeuille maintiendra l'état de révocation à l'index de la liste d'états référencé dans le champ 'status';

— la revendication 'exp' définie à l'appendice D de la spécification OID4VCI.

— *REMARQUE* concernant la valeur 'idx' dans la revendication 'key_storage_status.status' d'une attestation de clé: lorsque le fournisseur de portefeuille utilise l'option 'type-shared index' (voir R_KA_1 ci-dessous), toutes les attestations de clé se rapportant au même type de WSCD ou de magasin de clés partagent le même index de la liste d'états. Par conséquent, la valeur 'idx' n'est pas unique pour chaque unité de portefeuille. À l'inverse, lorsque le fournisseur de portefeuille utilise l'option 'per-key-attestation index', la valeur 'idx' est unique pour chaque unité de portefeuille (ou unique en mode 'pairwise' pour chaque émetteur de justificatifs d'identité). Toutefois, dans tous les cas, un émetteur de justificatifs d'identité ne doit pas utiliser la valeur 'idx' dans une attestation de clé comme identifiant d'unité de portefeuille, mais doit utiliser plutôt la valeur 'idx' dans une attestation d'instance de portefeuille.

— C_KA-2: lorsqu'une attestation de clé est envoyée dans un type de preuve 'attestation', elle doit également comprendre un c_nonce valide, tel que défini à l'appendice F.3 de la spécification OID4VCI.

— C_KA-3: un émetteur de justificatifs d'identité ne doit pas interpréter le paramètre 'exp' au niveau le plus élevé d'une attestation de clé comme étant la fin de la période de maintien de la révocation du WSCD ou du magasin de clés.

— *REMARQUE:* le paramètre 'exp' au niveau le plus élevé d'une attestation de clé indique à quel moment l'attestation de clé proprement dite expire.

d) Exigences relatives au cycle de vie

— La présente annexe spécifie les paramètres de métadonnées suivants de l'émetteur de justificatifs d'identité:

— 'preferred_client_status_period': FACULTATIF. Un nombre entier indiquant la durée restante préférée de maintien de l'état de l'attestation d'instance de portefeuille à présenter par l'unité de portefeuille lors de la délivrance, en secondes. La durée restante de maintien de l'état est définie comme la valeur de 'client_status.exp' dans l'attestation, moins l'heure de réception de l'attestation.

— 'preferred_key_storage_status_period': FACULTATIF. Un nombre entier indiquant la durée restante préférée de maintien de l'état de l'attestation de clé à présenter par l'unité de portefeuille lors de la délivrance, en secondes. La durée restante de maintien de l'état est définie comme la valeur de 'key_storage_status.exp' dans l'attestation, moins l'heure de réception de l'attestation.

— LC_WIA-1: un serveur d'autorisation peut communiquer ses préférences en ce qui concerne la durée restante de maintien de l'état dans les attestations d'instance de portefeuille en intégrant le paramètre de métadonnées 'preferred_client_status_period' dans son point de terminaison de métadonnées d'émetteur de justificatifs d'identité, comme indiqué à la section 12.2.2 de la spécification OID4VCI.

— LC_WIA-1.1: ce champ doit être placé au niveau le plus élevé des métadonnées de l'émetteur de justificatifs d'identité.

— LC_WIA_2: un serveur d'autorisation ne doit pas interpréter le paramètre 'exp' au niveau le plus élevé d'une attestation d'instance de portefeuille comme étant la fin de la période de maintien de la révocation de l'instance de portefeuille.

— LC_WIA_3: lorsqu'un fournisseur de portefeuille appose sa signature ou son cachet sur une attestation d'instance de portefeuille, il doit maintenir l'état de révocation de l'instance de portefeuille concernée jusqu'à ce que la 'wallet_instance_status.exp' indiquée dans cette attestation d'instance de portefeuille soit écoulée.

— LC_KA-1: si une attestation de clé est nécessaire, un émetteur de justificatifs d'identité peut communiquer ses préférences en ce qui concerne la durée restante de maintien de l'état dans les attestations de clé en intégrant le paramètre de métadonnées spécifié plus haut 'preferred_key_storage_status_period' dans son point de terminaison de métadonnées d'émetteur de justificatifs d'identité, comme indiqué à la section 12.2.2 de la spécification OID4VCI.

— LC_KA-1.1: ce champ doit être placé à l'intérieur de l'objet 'key_attestations_required' comme indiqué à la section 12.2.4 de la spécification OID4VCI.

— LC_KA-2: un fournisseur de portefeuille doit choisir la période de validité technique des attestations de clé qu'il délivre.

— LC_KA-3: lorsqu'un fournisseur de portefeuille appose sa signature ou son cachet sur une attestation de clé, il doit maintenir l'état de révocation du WSCD ou du magasin de clés jusqu'à ce que la 'key_storage_status.exp' indiquée dans cette attestation de clé soit écoulée.

— LC_GEN-1: un fournisseur de portefeuille doit veiller à ce qu'une unité de portefeuille puisse toujours présenter des attestations d'unité de portefeuille et des attestations de clé dont les 'client_status.exp' et 'key_storage_status.exp' (respectivement) sont situées au moins 31 jours plus tard au moment de leur présentation à un serveur d'autorisation ou à un émetteur de justificatifs d'identité.

— *REMARQUE:* cela garantit que les fournisseurs de données d'identification personnelle peuvent s'appuyer sur un chaînage de révocation sans être contraints de délivrer des données d'identification personnelle à courte durée de vie.

— LC_GEN-2: un fournisseur de portefeuille doit veiller à ce qu'une unité de portefeuille récupère les métadonnées de l'émetteur de justificatifs d'identité lors de la délivrance.

  — LC_GEN_2.1: si un champ 'preferred_key_storage_status_period' est inclus dans ces métadonnées, l'unité de portefeuille doit envoyer une attestation de clé pour laquelle la valeur ('key_storage_status.exp' − date actuelle) − 'preferred_key_storage_status_period' est la plus proche possible de zéro sans être négative. Si l'unité de portefeuille ne dispose pas d'une telle attestation de clé, elle doit obtenir du fournisseur de portefeuille une nouvelle attestation de clé qui satisfait à la condition 'key_storage_status.exp' − date actuelle ≥ 'preferred_key_storage_status_period'.

  — LC_GEN_2.2: si un champ 'preferred_client_status_period' est inclus dans ces métadonnées, l'unité de portefeuille doit envoyer une attestation d'instance de portefeuille pour laquelle la valeur ('client_status.exp' − date actuelle) − 'preferred_client_status_period' est la plus proche possible de zéro sans être négative. Si l'unité de portefeuille ne dispose pas d'une telle attestation d'instance de portefeuille, elle doit obtenir du fournisseur de portefeuille une nouvelle attestation d'instance de portefeuille qui satisfait à la condition 'client_status.exp' − date actuelle ≥ 'preferred_client_status_period'.

— LC_GEN-3: la période de validité technique des données d'identification personnelle doit prendre fin avant le 'client_status.exp' de l'attestation d'instance de portefeuille et avant le 'key_storage_status.exp' de l'attestation de clé envoyées au fournisseur de données d'identification personnelle lors du processus de délivrance.

— LC_GEN-4: un fournisseur de données d'identification personnelle ayant une période de validité technique de plus de 24 heures doit vérifier l'état de révocation de l'attestation d'instance de portefeuille et de l'attestation de clé reçues lors de la délivrance au moins une fois toutes les 24 heures pendant la période de validité technique des données d'identification personnelle. Lorsque l'une ou l'autre de ces attestations est révoquée, le fournisseur doit révoquer les données d'identification personnelle.

e) Exigences en matière de révocation

— R_GEN-1: un fournisseur de portefeuille doit utiliser des listes d'états des jetons (définies dans la spécification Token Status List de l'IETF) comme mécanisme de révocation tant pour les attestations de clé que pour les attestations d'instance de portefeuille, comme indiqué respectivement dans les appendices D et E de la spécification OID4VCI.

— *REMARQUE:* pour améliorer la modularité de ses listes d'états, un fournisseur de portefeuille peut recourir aux optimisations suivantes:

  — diviser la liste d'états en plusieurs sections, lorsque les fournisseurs de portefeuille comptent un nombre important d'utilisateurs et d'attestations délivrées. Il existe beaucoup de stratégies de sectionnement, fondées par exemple sur une taille fixe ou sur une période donnée. La stratégie de sectionnement est laissée à l'appréciation du fournisseur de portefeuille. Les critères à prendre en considération peuvent comprendre la taille des listes d'états à télécharger et le respect de la vie privée de l'utilisateur;

  — prévoir plusieurs listes d'états;

  — comprimer les listes d'états pour en réduire la taille.

— R_WIA-1: un fournisseur de portefeuille peut attribuer la même valeur à la revendication 'idx' dans la revendication 'client_status.status' de toutes les attestations d'instance de portefeuille qu'une unité de portefeuille donnée présente au même serveur d'autorisation. Cette option est appelée 'per-issuer reuse'. Si cette option est utilisée, les conditions suivantes s'appliquent:

  — R_WIA-1.1: l'unité de portefeuille doit conserver la trace de la valeur d'index qu'elle a utilisée pour chaque serveur d'autorisation avec lequel elle a précédemment interagi et doit demander une attestation d'instance de portefeuille contenant cette même valeur d'index lorsqu'elle interagit à nouveau avec le même serveur d'autorisation.

  — R_WIA-1.2: lorsqu'un fournisseur de portefeuille reçoit une demande d'attestation d'instance de portefeuille contenant une valeur d'index spécifique, il doit vérifier que l'unité de portefeuille à l'origine de la demande a reçu cette valeur d'index au préalable avant de délivrer une nouvelle attestation d'instance de portefeuille avec cette valeur d'index.

  — R_WIA-1.3: l'unité de portefeuille ne doit pas réutiliser la même valeur d'index pour ses interactions avec d'autres serveurs d'autorisation.

— *REMARQUE:* si l'option 'per-issuer reuse' est utilisée, le fournisseur de portefeuille sera en mesure de déterminer le nombre de serveurs d'autorisation avec lesquels une unité de portefeuille a interagi et la fréquence à laquelle elle interagit avec chacun d'eux.

— R_WIA-2: dans sa politique relative au respect de la vie privée, le fournisseur de portefeuille doit indiquer s'il utilise l'option 'per-issuer reuse' pour la révocation des instances de portefeuille.

— R_WIA-3: si un fournisseur de portefeuille n'utilise pas l'option 'per-issuer reuse', il doit attribuer une valeur d'index nouvelle et non associable à chaque attestation d'instance de portefeuille qu'il délivre.

— R_WIA-4: si une unité de portefeuille doit être révoquée, le fournisseur de portefeuille doit révoquer les valeurs d'index dans la revendication 'client_status.statu' de toutes les attestations d'instance de portefeuille associées à cette unité de portefeuille.

— R_WIA-5: un fournisseur de portefeuille doit tenir compte de l'échelle de son déploiement et de l'architecture sous-jacente lorsqu'il détermine la taille des listes d'états de ses attestations d'instance de portefeuille, en veillant à ce qu'elles soient suffisamment grandes pour empêcher la corrélation et protéger la vie privée des utilisateurs. Dans la mesure du possible, une liste d'états doit se rapporter au minimum à 10 000 attestations.

— R_KA_1: un fournisseur de portefeuille doit choisir l'une des options d'assignation d'index suivantes pour la revendication 'key_storage_status.status' dans une attestation de clé:

  — option 1, appelée 'type-shared index', dans laquelle toutes les attestations de clé attestant des clés stockées dans le même type de WSCD ou de magasin de clés contiennent la même valeur d'index dans 'key_storage_status.status';

  — option 2, appelée 'per-key-attestion index', dans laquelle une attestation de clé attestant des clés stockées dans un WSCD donné ou un magasin de clés donné contient une valeur d'index unique (pairwise) dans 'key_storage_status.status'.

— *REMARQUE:* lorsqu'un fournisseur de portefeuille utilise l'option 1, une action de révocation unique annule toutes les attestations de clés du type concerné pour toutes les unités de portefeuille. En outre, étant donné que toutes les attestations de clé pour un même type de WSCD ou de magasin de clés partagent un index unique de la liste d'états, le nombre d'entrées dans cette liste pour une attestation de clé correspond au nombre de types de WSCD ou de magasins de clés pris en charge par le fournisseur de portefeuille, et non au nombre d'unités de portefeuille déployées. Par conséquent, les considérations relatives à la protection de la vie privée qui motivent la taille minimale de la liste d'états dans le cas des instances de portefeuille ne s'appliquent pas aux listes d'états des attestations de clé dans le cadre de l'option 1, à condition qu'un nombre suffisant d'unités de portefeuille utilise le même type de WSCD ou de magasin de clés.

— *REMARQUE:* lorsqu'un fournisseur de portefeuille utilise l'option 2, chaque index représente l'état de révocation du WSCD ou du magasin de clés spécifique attesté dans cette attestation de clé.

— *REMARQUE:* lorsqu'un fournisseur de portefeuille utilise l'option 2, un WSCD ou un magasin de clés spécifique peut également être révoqué à la demande de l'utilisateur.

— R_KA-2: lorsqu'un fournisseur de portefeuille utilise l'option 2, il peut, à titre facultatif, utiliser l'option 'per-issuer reuse' décrite dans le paragraphe R_WIA-1. Si le fournisseur de portefeuille utilise cette option, les exigences des paragraphes R_WIA-1 à R_WIA-3 s'appliquent par analogie.

— R_KA-3: si un fournisseur de portefeuille utilise l'option 2, il doit tenir compte de l'échelle de son déploiement et de l'architecture sous-jacente lorsqu'il détermine la taille des listes d'états de ses attestations de clé, en veillant à ce qu'elles soient suffisamment grandes pour empêcher la corrélation et protéger la vie privée des utilisateurs. Dans la mesure du possible, une liste d'états doit se rapporter au minimum à 10 000 attestations de clé.

— R_KA-4: si un fournisseur de portefeuille utilise l'option 1 ('type-shared index'), il ne doit révoquer une entrée 'key_storage_status.status' que si le type de WSCD ou de magasin de clés présente une vulnérabilité en matière de sécurité.

f) Exigences relatives aux algorithmes de signature

— SA-1: pour signer les attestations d'instance de portefeuille, les attestations de clé, les preuves de possession connexes et les listes d'états des jetons, l'un des algorithmes suivants doit être utilisé:

  — ES256 (ECDSA avec SHA-256 et P-256)

  — ES384 (ECDSA avec SHA-384 et P-384)

  — ES512 (ECDSA avec SHA-512 et P-521)

— SA-2: un fournisseur de portefeuille doit choisir lequel des algorithmes mentionnés dans le paragraphe SA-1 il utilisera.

— SA-3: un serveur d'autorisation ou un émetteur de justificatifs d'identité (tels que définis dans la spécification OID4VCI) doit prendre en charge tous les algorithmes mentionnés dans le paragraphe SA-1.».

ANNEXE IV

«ANNEXE II

Liste des normes visées à l'article 8

Les spécifications techniques énoncées dans les paragraphes 2 à 6 d'ETSI TS 119 472-1 V1.2.1 (2026-02) s'appliquent, moyennant les adaptations suivantes:

1) 2.1. Références normatives

— [16] ETSI EN 319 412-1 V1.6.1 (2025-06): "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures (Signatures électroniques et infrastructures de confiance (ESI) - profils de certificat; partie 1: présentation générale et structures de données communes)".

— [17] ETSI TS 119 412-6 V1.1.1 (2025-09): "Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 6: Certificate profile requirements for PID, Wallet, EAA, QEAA, and PSBEAA providers [Signatures électroniques et infrastructures de confiance (ESI); profils de certificat; partie 6: Exigences applicables aux profils de certificats pour les fournisseurs de données d'identification personnelle (PID), de portefeuilles, d'attestations électroniques d'attributs (EAA), d'attestations électroniques qualifiées d'attributs (QEAA) et d'attestations électroniques d'attributs délivrées par un organisme du secteur public (PSBEAA)]".

— [25] Token Status List (TSL) de l'IETF, draft-ietf-oath-status-list-20: "Token Status List", 20 avril 2026.

2) 4.2.11.1 General requirements

— EAA-4.2.11.1-06: lorsqu'un élément d'état est utilisé pour des données d'identification personnelle, des attestations électroniques qualifiées d'attributs ou des attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte, il indique uniquement si l'attestation est révoquée ou non et ne prend en charge aucune autre valeur d'état telle que la suspension.

— EAA-4.2.11.1-06.1: lorsqu'une attestation est révoquée, sa révocation est permanente.

3) 4.2.13 EAA short-lived

— EAA-4.2.13-03: lorsque des attestations électroniques d'attributs à faible durée de validité sont délivrées pour 24 heures ou moins, aucune révocation n'est exigée.

4) 4.6.3. Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (PuB-EAA)

— PuB-EAA-4.6.2-03: vide.

— Pub-EAA-4.6.2-04: vide.

— PuB-EAA-4.6.3-03: La signature numérique PuB-EAA devrait contenir le certificat qualifié à l'appui de la signature numérique PuB-EAA.

— PuB-EAA-4.6.3-04: Le certificat qualifié à l'appui de la signature numérique PuB-EAA doit satisfaire aux exigences du paragraphe 8 d'ETSI TS 119 412-6 v1.1.1 et doit contenir le QcType qcStatement tel que défini dans ETSI EN 319 412-5 v2.5.1, la valeur id-etsi-qct-eidaspsbeaa étant définie comme suit:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER: = {id-etsi-eidas2-qct-extensions 3} — Certificat visé à l'article 45 *septies*, paragraphe 1, point b), à l'appui de la signature électronique qualifiée ou du cachet électronique qualifié de l'organisme du secteur public visé à l'article 3, point 46), du règlement (UE) n° 910/2014.

5) 5.2.10.1 General requirements

— EAA-5.2.10.1-04: vide.

— EAA-5.2.10.1-05: vide.

— EAA-5.2.10.1-06: Le membre "status" peut contenir le membre "status_list" comme indiqué au paragraphe 6.2 du projet draft-ietf-oauth-status-list-20 de l'IETF[25].

— EAA-5.2.10.1-07: vide.

— EAA-5.2.10.1-08: vide.

— EAA-5.2.10.1-09: vide.

— EAA-5.2.10.1-10: vide.

— EAA-5.2.10.1-11: vide.

— EAA-5.2.10.1-12: vide.

6) 6.2.10.1 General requirements

— EAA-6.2.10.1-01: lorsqu'une attestation électronique d'attributs conforme à la norme ISO/IEC mdoc utilise le mécanisme de liste d'états d'attestations tel que défini dans EAA-6.2.10.1-02.2 ou le mécanisme de liste de révocation d'attestations tel que défini dans EAA-6.2.10.1-02.3, son objet de sécurité mobile (MSO) contient la structure d'état, telle que spécifiée dans EAA-6.2.10.1-17, qui contient les informations de révocation du MSO.

— EAA-6.2.10.1-01.1: lorsque l'élément d'état met en œuvre le mécanisme de liste d'identifiants, il contient l'élément identifier_list figurant dans EAA-6.2.10.1-11.

— EAA-6.2.10.1-01.2: lorsque l'élément d'état met en œuvre le mécanisme de liste d'états, il contient l'élément status_list figurant dans EAA-6.2.10.1-13.

— *REMARQUE:*

  — La structure d'état contient une référence à une liste de révocation de MSO.

  — La liste de révocation de MSO est une structure COSE_Sign1 qui indique si un MSO donné est révoqué ou non.

  — La structure d'état contient toutes les informations nécessaires pour permettre à la partie utilisatrice de portefeuille de déterminer si la liste de révocation de MSO est authentique.

— EAA-6.2.10.1-02: le fournisseur de données d'identification personnelle, le fournisseur d'attestations électroniques d'attributs qualifiées ou le fournisseur d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte utilise l'une des méthodes suivantes pour la révocation des données d'identification personnelle, des attestations électroniques d'attributs qualifiées ou des attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte:

— EAA-6.2.10.1-02.1: lorsqu'il délivre des attestations électroniques d'attributs à faible durée de validité pour une période inférieure ou égale à 24 heures, la révocation n'est pas nécessaire.

— EAA-6.2.10.1-02.2: utiliser un mécanisme de liste d'états d'attestation pour encoder les informations de révocation sous forme de liste d'états.

— EAA-6.2.10.1-02.2.1: le mécanisme de liste d'états révoque un MSO si le bit de la position de bit définie par l'émetteur dans le MSO est activé dans la liste d'états.

— EAA-6.2.10.1-02.2.2: le mécanisme de liste d'états est précisé dans la spécification relative à la liste d'états des jetons (draft-ietf-oauth-status-list-20).

— EAA-6.2.10.1-02.3: utiliser un mécanisme de liste de révocation d'attestations pour encoder les informations de révocation sous forme de liste d'identifiants.

— EAA-6.2.10.1-02.3.1: le mécanisme de liste d'identifiants révoque un MSO si l'identifiant défini par l'émetteur dans le MSO figure sur la liste d'identifiants.

— EAA-6.2.10.1-02.3.2: EAA-6.2.10.1-06, EAA-6.2.10.1-08, EAA-6.2.10.1-09, EAA-6.2.10.1-10 et EAA-6.2.10.1-11 précisent le mécanisme de liste d'identifiants, sur la base des exigences de la spécification relative à la liste d'états des jetons, y compris les points communs entre le mécanisme de liste d'états et le mécanisme de liste d'identifiants.

— EAA-6.2.10.1-03: lorsqu'un élément d'état est utilisé pour des données d'identification personnelle, des attestations électroniques qualifiées d'attributs ou des attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte, l'état "révoqué" doit être utilisé exclusivement.

— EAA-6.2.10.1-03.1: pour une liste d'états, cela signifie que seules les valeurs 'valid' et 'invalid', telles que précisées dans la spécification relative à la liste d'états des jetons, doivent être utilisées.

— EAA-6.2.10.1-03.2: pour la liste d'identifiants, seuls les MSO révoqués, par opposition aux MSO provisoirement suspendus, doivent être inscrits sur la liste d'identifiants.

— EAA-6.2.10.1-04: lorsqu'un MSO est révoqué, sa révocation est permanente.

— EAA-6.2.10.1-05: la vérification de la liste de révocation du MSO est facultative pour la partie utilisatrice de portefeuille et, le cas échéant, la vérification doit être conforme aux exigences de vérification précisées dans la spécification relative à la liste d'états des jetons et la spécification relative à la structure d'état énoncée dans EAA-6.2.10.1-01.

— EAA-6.2.10.1-05.1: lorsqu'une partie utilisatrice de portefeuille doit être en mesure de vérifier l'état de révocation des données d'identification personnelle ou des attestations électroniques d'attributs, elle doit prendre en charge à la fois le mécanisme de liste d'états d'attestations et le mécanisme de liste de révocation d'attestations prévus dans EAA-6.2.10.1-02.

— EAA-6.2.10.1-06: le identifier_list et le status_list du MSO peuvent contenir l'élément de certificat.

— EAA-6.2.10.1-06.1: lorsque l'élément de certificat est présent, il doit contenir un certificat contenant la clé publique ayant apposé la signature ou le cachet sur le certificat de plus haut niveau dans l'élément x5chain de la structure de liste de révocation du MSO.

— EAA-6.2.10.1-06.1.1: la partie utilisatrice de portefeuille doit utiliser ce certificat comme ancre de confiance pour vérifier l'élément x5chain de la structure de liste de révocation du MSO.

— EAA-6.2.10.1-06.2: en l'absence d'élément de certificat, le certificat avec lequel a été signé le certificat dans l'élément x5chain du MSO doit être utilisé pour apposer la signature ou le cachet sur le certificat de niveau supérieur dans l'élément x5chain de la structure de liste de révocation du MSO.

— EAA-6.2.10.1-06.2.1: l'instance de la partie utilisatrice de portefeuille doit utiliser ce certificat comme ancre de confiance pour vérifier l'élément x5chain de la structure de liste de révocation du MSO.

— EAA-6.2.10.1-07: conformément à la spécification de liste d'états des jetons, une liste de révocation du MSO doit être mise en œuvre sous forme de jeton de liste d'états au format CWT.

— EAA-6.2.10.1-08: pour la liste de révocation du MSO: pour le mécanisme de la liste d'identifiants et le mécanisme de liste d'états, les exigences applicables sont les suivantes:

  — la revendication exp doit être présente.

  — la revendication ttl doit être présente.

  — la revendication aggregation_uri dans la revendication IdentifierList ou StatusList peut être présente et le fournisseur de données d'identification personnelle, le fournisseur d'attestations électroniques qualifiées d'attributs ou le fournisseur d'attestations électroniques d'attributs délivrées par un organisme du secteur

public responsable d'une source authentique ou pour son compte peut utiliser la revendication aggregation_uri pour indiquer que le mécanisme d'agrégation tel que spécifié dans la spécification de la liste d'états des jetons est pris en charge.

— le CWT doit être un objet COSE_Sign1 utilisant l'un des algorithmes de signature suivants pour calculer la signature:

a) 'ES256' (ECDSA avec courbe NIST P-256 et SHA-256);

b) 'ES384' (ECDSA avec courbe NIST P-384 et SHA-384);

c) 'ES512' (ECDSA avec courbe NIST P-521 et SHA-512);

d) 'ESB256' (ECDSA avec courbe NIST brainpoolP256r1 et SHA-256);

e) 'ESB384' (ECDSA avec courbe NIST brainpoolP384r1 et SHA-384);

f) 'ESB512' (ECDSA avec courbe NIST brainpoolP512r1 et SHA-512);

— le CWT doit contenir la x5chain dans l'en-tête protégé qui contient le certificat ou la chaîne de certificats afin de vérifier la signature de la liste de révocation du MSO.

— l'utilisation étendue de la clé de l'identifiant d'objet précisé dans la spécification de la liste d'états des jetons peut servir au certificat de signature de la liste d'états et au certificat de signature de la liste d'identifiants et les instances de parties utilisatrices de portefeuille peuvent prendre en charge l'utilisation étendue de la clé des identifiants d'objet précisés dans la spécification de la liste d'états des jetons et pour l'identifiant d'objet, le fournisseur d'attestations électroniques d'attributs qualifiées ou le fournisseur d'attestations électroniques d'attributs délivrées par un organisme du secteur public ou pour son compte ne doivent pas rendre critique le champ d'utilisation étendue de la clé lorsqu'ils utilisent l'OID d'utilisation étendue de la clé précisé dans la spécification de la liste d'états des jetons.

— EAA-6.2.10.1-09: par dérogation aux exigences de la spécification de la liste d'états des jetons, pour le mécanisme de liste d'identifiants, les exigences applicables sont les suivantes:

— la valeur de la revendication type doit être 'application/identifierlist+cwt';

— la revendication StatusList ne doit pas être présente dans l'ensemble de revendications CWT;

— la structure IdentifierList définie dans EAA-6.2.10.1-11 doit être présente en tant que revendication dans l'ensemble de revendications CWT qui utilise la clé 65530.

— EAA-6.2.10.1-10: la structure IdentifierList doit être une structure CBOR avec le CDDL suivant:

```
IdentifierList = {

    'identifiers': { * Identifier => IdentifierInfo },

    ? 'aggregation_uri': Aggregation_uri

    * tstr => RFU

}

IdentifierInfo = { tstr/int => RFU }

Identifier = bstr

Aggregation_uri = tstr
```

— EAA-6.2.10.1-10.1: lorsque l'identifiant dans la IdentifierList est présent, le MSO qui contient l'identifiant dans l'élément d'état est révoqué.

— EAA-6.2.10.1-10.2: la revendication aggregation_uri est précisée dans la section 9.2 de la spécification de la liste d'états des jetons.

— EAA-6.2.10.1-10.3: le type de contenu de la liste d'identifiants doit être 'application/identifierlist+cwt' tel qu'énoncé dans les exigences figurant dans la section 8.2 de la spécification de la liste d'états des jetons.

— EAA-6.2.10.1-11: les exigences applicables à l'élément identifier_list dans le MSO sont les suivantes (voir EAA-6.2.10.1-17).

— EAA-6.2.10.1-11.1: l'élément identifier_list est une structure CBOR avec le CDDL suivant:

```
IdentifierListInfo = {

        'id': Identifier ,

        'uri': URI,

        ? 'certificate': Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: pour éviter toute éventuelle utilisation de l'identifiant comme corrélation dans différentes présentations, il doit être unique pour chaque MSO.

— EAA-6.2.10.1-12: les exigences applicables à la liste d'états sont les suivantes:

  — EAA-6.2.10.1-12.1: l'élément bits de la structure de StatusList doit être fixé à 1.

— EAA-6.2.10.1-13: les exigences applicables à l'élément status_list dans le MSO sont les suivantes (voir EAA-6.2.10.1-17).

  — EAA-6.2.10.1-13.1: l'élément status_list doit respecter les exigences applicables à la structure StatusListInfo précisées dans la spécification relative à la liste d'états des jetons et l'élément de certificat facultatif défini dans EAA-6.2.10.1-06 doit être ajouté.

  — EAA-6.2.10.1-13.2: pour éviter toute éventuelle utilisation de l'index d'état comme corrélation dans différentes présentations, chaque MSO doit avoir une combinaison d'index d'état et d'URI unique.

— EAA-6.2.10.1-14: le fournisseur de portefeuille doit utiliser la deuxième (EAA-6.2.10.1-02.2) ou la troisième (EAA-6.2.10.1-02.3) des méthodes spécifiées dans EAA-6.2.10.1-02 pour la révocation d'une attestation d'instance de portefeuille (WIA) et pour la révocation d'une attestation de clé (KA).

— EAA-6.2.10.1-15: le fournisseur de portefeuille met en œuvre les mécanismes de révocation d'attestation spécifiés dans EAA-6.2.10.1-02 dans sa solution de portefeuille.

— EAA-6.2.10.1-16: le fournisseur de données d'identification personnelle et le fournisseur d'attestations électroniques d'attributs doivent prendre en charge à la fois le mécanisme de liste d'états d'attestations et le mécanisme de liste de révocation d'attestations spécifiés dans EAA-6.2.10.1-02 pour vérifier l'état de révocation d'une attestation d'instance de portefeuille (WIA) et d'une attestation de clé (KA).

— EAA-6.2.10.1-17: la structure d'état dans le MSO doit être une structure CBOR avec le CDDL suivant:

Status = {

? 'identifier_list' : IdentifierListInfo,

? 'status_list': StatusListInfo,

* tstr => RFU

}»

ANNEXE V

«ANNEXE III

Spécifications techniques visées à l'article 10

— Spécifications techniques:

  — paragraphe 4.2.5 de l'ETSI TS 119 472-3 V1.1.1 (2026-03).»

ANNEXE VI

L'annexe IV du règlement d'exécution (UE) 2024/2979 est modifiée comme suit:

1) Le point 1 est remplacé par le texte suivant:

«1. Format de signature ou de cachet obligatoire:

a) PAdES (PDF Advanced Electronic Signature) comme spécifié dans ETSI EN 319 142-1 V1.2.1 (2024-01); "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures [Signatures électroniques et infrastructures de confiance (ESI) - Signatures numériques PAdES; partie 1: blocs de base et signatures de référence PAdES]."».

2) Le point 3 est remplacé par le texte suivant:

«3. Interface de programmation d'application:
ETSI TS 119 432 v1.3.1 (2026-03) paragraphes 6.4.3, A.6, A.7 et A.8.».

ANNEXE VII

«*ANNEXE VI*

Label de confiance de l'UE pour le portefeuille d'identité numérique en couleur



»

ANNEXE VIII

«*ANNEXE VII*

Label de confiance de l'UE pour le portefeuille d'identité numérique en noir et blanc



»

ANNEXE IX

«ANNEXE VIII

Données du label de confiance de l'UE pour le portefeuille d'identité numérique

Données	Description	Encodage	Statut
TrustMarkResourceURL	URL des ressources graphiques du label de confiance de l'UE pour le portefeuille d'identité numérique et des ressources d'information des utilisateurs dans l'interface utilisateur du portefeuille.	URL	Obligatoire
ListOfCertifiedWalletsURL	URL de la liste publique des solutions de portefeuille certifiées dans l'UE, telle que prévue par le règlement d'exécution (UE) 2025/849 de la Commission ([1]).	URL	Obligatoire
ListOfCertifiedWalletsQRCode	Code QR contenant les informations de ListOfCertifiedWalletsURL	ISO-8859-1 Byte mode QR code	Facultatif
WalletSolutionInfoPageURL	URL de la page d'information de la solution de portefeuille certifiée de ListOfCertifiedWalletsURL complétée par un '?' et l'identifiant WalletSolutionID de la solution de portefeuille.	URL	Obligatoire
WalletSolutionInfoPageQRCode	Code QR contenant les informations de WalletSolutionInfoPageURL	ISO-8859-1 Byte mode QR code	Facultatif
WalletVerifierToolURL *	URL renvoyant au point de terminaison de l'outil de vérification du portefeuille */.well-known/openid-credential-issuer* utilisé pour extraire les métadonnées du fournisseur d'attestation.	URL	Facultatif

([1]) Règlement d'exécution (UE) 2025/849 de la Commission du 6 mai 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne la communication à la Commission et au groupe de coopération d'informations destinées à la liste des portefeuilles européens d'identité numérique certifiés (JO L, 2025/849, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj).»

ANNEXE X

L'annexe II du règlement d'exécution (UE) 2024/2980 est modifiée comme suit:

1) à l'annexe II, section 1, le point 1), i), est remplacé par le texte suivant:

«i) un ou plusieurs certificats conformes à la norme ETSI EN 319 412-2 V2.4.1 (2025-06) ou à la norme ETSI EN 319 412-3 V1.3.1 (2023-09) qui peuvent être utilisés pour vérifier la signature ou le cachet créés par le bureau d'enregistrement concernant les informations du registre, et pour lesquels les données d'identité certifiées comprennent le nom du bureau d'enregistrement et, le cas échéant, son numéro d'immatriculation, comme prévu respectivement aux points c) et d);»;

2) à l'annexe II, section 2, le point 1), h), est remplacé par le texte suivant:

«h) un ou plusieurs certificats conformes à la norme ETSI EN 319 412-2 V2.4.1 (2025-06) ou à la norme ETSI EN 319 412-3 V1.3.1 (2023-09) qui peuvent être utilisés pour authentifier et valider les attestations d'unité de portefeuille délivrées par le fournisseur de portefeuille, et pour lesquels les données d'identité certifiées comprennent le nom du fournisseur de portefeuille et, le cas échéant, son numéro d'immatriculation, comme prévu respectivement aux points a) et b);»;

3) à l'annexe II, section 3, le point 1), h), est remplacé par le texte suivant:

«h) un ou plusieurs certificats conformes à la norme ETSI EN 319 412-2 V2.4.1 (2025-06) ou à la norme ETSI EN 319 412-3 V1.3.1 (2023-09) qui peuvent être utilisés pour vérifier la signature ou le cachet créés par le fournisseur de données d'identification personnelle concernant les données d'identification personnelle qu'il fournit, et pour lesquels les données d'identité certifiées comprennent le nom du fournisseur de données d'identification personnelle et, le cas échéant, son numéro d'immatriculation, comme prévu respectivement aux points a) et b).»;

4) à l'annexe II, section 4, le point 1), g), est remplacé par le texte suivant:

«g) un ou plusieurs certificats conformes à la norme ETSI EN 319 412-2 V2.4.1 (2025-06) ou à la norme ETSI EN 319 412-3 V1.3.1 (2023-09) qui peuvent être utilisés pour vérifier la signature ou le cachet créés par le fournisseur de certificats d'accès de partie utilisatrice de portefeuille sur les certificats d'accès qu'il fournit aux parties utilisatrices de portefeuille avec, le cas échéant, les informations nécessaires pour distinguer les certificats d'accès de partie utilisatrice de portefeuille d'autres certificats.»;

5) à l'annexe II, la section 5 suivante est ajoutée:

«5. Notifications d'informations concernant les fournisseurs de certificats d'enregistrement de partie utilisatrice de portefeuille

1. Les États membres transmettent à la Commission les informations suivantes concernant les fournisseurs de certificats d'enregistrement de partie utilisatrice de portefeuille:

a) le nom du fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille;

b) le cas échéant, le numéro d'immatriculation du fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille;

c) l'État membre dans lequel le fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille est établi;

d) l'adresse électronique et le numéro de téléphone auxquels le fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille est joignable pour des questions relatives aux certificats d'enregistrement qu'il fournit aux parties utilisatrices de portefeuille;

e) le cas échéant, l'adresse URL de la page web du fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille contenant des informations supplémentaires sur le fournisseur et les certificats d'enregistrement qu'il fournit aux parties utilisatrices de portefeuille;

f) l'adresse URL de la page web où figurent les politiques et les conditions applicables à la fourniture et à l'utilisation des certificats d'enregistrement qu'il fournit aux parties utilisatrices de portefeuille;

g) un ou plusieurs certificats conformes à la norme ETSI EN 319 412-2 V2.4.1 (2025-06) ou à la norme ETSI EN 319 412-3 V1.3.1 (2023-09) qui peuvent être utilisés pour vérifier la signature ou le cachet créés par le fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille sur les certificats d'enregistrement qu'il fournit aux parties utilisatrices de portefeuille avec, le cas échéant, les informations nécessaires pour distinguer les certificats d'enregistrement de partie utilisatrice de portefeuille d'autres certificats.

2. Les informations visées au point 1 sont transmises pour chaque fournisseur de certificats d'enregistrement de partie utilisatrice de portefeuille.».

ANNEXE XI

«ANNEXE I

Protocoles et interfaces visés à l'article 4

La spécification technique ETSI TS 119 472-3 V1.1.1 (2026-03) s'applique moyennant les adaptations suivantes:

1) 4.1. General requirements

— GEN-REQ-4.1-05: vide.

— *REMARQUE:* vide.

2) 4.2.3. Provision of registration certificates of PID/EAA Provider to EUDI Wallet

— ISS-MDATA-REG_CERT-4.2.3-04: L'un des éléments du paramètre de tableau issuer_info contient le certificat d'enregistrement du fournisseur de PID/EAA.

— ISS-MDATA-REG_CERT-4.2.3-07: vide.

— ISS-MDATA-REG_CERT-4.2.3-08: vide.

— ISS-MDATA-REG_CERT-4.2.3-09: vide.

— ISS-MDATA-REG_CERT-4.2.3-10: vide.

— ISS-MDATA-REG_CERT-4.2.3-11: vide.

— ISS-MDATA-REG_CERT-4.2.3-12: vide.

— ISS-MDATA-REG_CERT-4.2.3-13: vide.

3) 4.2.4.2 ARF pre-defined PID/EAA reuse policy

— ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: lorsque le membre id a la valeur 'arf_annex_ii' et que le tableau associé à l'étiquette 'details' contient la valeur 'once_only' ou la valeur 'per relying-party', l'objet JSON qui contient ce tableau associé à l'étiquette 'details' doit aussi contenir un numéro JSON associé à l'étiquette 'reissue_trigger_unused'.

4) L'annexe A ne s'applique pas.».

ANNEXE XII

«ANNEXE II

Spécifications techniques visées à l'article 5

Les spécifications techniques de l'annexe C de la norme ISO/IEC 18013-7: 2025 s'appliquent.

Les spécifications techniques des paragraphes 4.1, 4.2, 5 et 6 de la norme ETSI TS 119 472-2 V1.2.1 (2026-03) s'appliquent moyennant les adaptations suivantes, notamment l'insertion d'un nouveau paragraphe 4.3:

1) 1. Champ d'application

— Le présent document spécifie deux profils de protocoles permettant aux parties utilisatrices (RP) de demander des EAAP ou des données d'identification personnelle (PID) au portefeuille européen d'identité numérique, et au portefeuille européen d'identité numérique d'envoyer à la RP les EAAP/PID demandées. Chacun de ces profils prend en charge deux mécanismes de transmission, à savoir: avec médiation d'API et sans médiation d'API, comme suit:

a) Un profil se fonde sur:

— ISO/IEC 18013-5 [10] pour le mécanisme de transmission sans médiation d'API uniquement, et

— sur l'annexe C de la norme ISO/IEC 18013-7 [16] pour le mécanisme de transmission avec médiation d'API.

Ce profil est appelé profil ISO/IEC-mdoc et il est défini au paragraphe 5 du présent document.

b) Un profil se fonde sur:

OpenID4VC-HAIP [11] à la fois pour les mécanismes de transmission avec médiation d'API et sans médiation d'API, comme suit:

— les sections 5, 5.1, 5.3, 7 et 8 de [11] pour la transmission via Redirects ou un mécanisme de transmission sans médiation d'API, et

— les sections 5, 5.2, 5.3, 7 et 8 de [11] pour la transmission par un mécanisme de transmission avec médiation d'API.

Ce profil est appelé profil OpenID4VC-HAIP et il est défini au paragraphe 6 du présent document.

2) 2.1. Références normatives

— [15] ISO 639: 'Language code'

— [16] ISO/IEC 18013-7: 2025 'Personal identification – ISO – compliant driving licence – Part 7: Mobile driving licence (mDL) add-on functions' (Identification des personnes – Permis de conduire conforme à l'ISO – Partie 7: Fonctionnalités supplémentaires pour permis de conduire sur téléphone mobile).

3) 4.1. EAAP implementation based on SD-JWT VC

— EAAP-SD-JWT VC-04: vide.

4) 4.2. EAAP implementation based on ISO/IEC-mdoc

— EAAP-ISO/IEC-mdoc-01: vide.

— *Remarque 2:* vide.

— EAAP-ISO/IEC-mdoc-02: vide.

5) 4.3. EAAP implementation with mediating API

— EAAP-API-GEN-01: le portefeuille européen d'identité numérique prend en charge une API de médiation qui accepte les deux protocoles définis au paragraphe 5.2 du [11] et à l'annexe C du [16].

— *REMARQUE:* lorsque l'appareil sur lequel le portefeuille européen d'identité numérique est installé ne prend pas en charge les deux protocoles, cette exigence ne peut pas être satisfaite, ce qui entraîne une non-conformité due au fait que les systèmes d'exploitation et navigateurs sous-jacents ne mettent pas en œuvre les caractéristiques d'interopérabilité nécessaires.

— EAAP-API-GEN-02: le portefeuille européen d'identité numérique prend en charge une API de médiation au moins pour les types de PID et d'EAA enregistrés dans le catalogue de programmes tel que défini dans le règlement d'exécution (UE) 2025/1569, et au moins pour tous les formats définis à l'annexe II du règlement d'exécution (UE) 2024/2979.

— *REMARQUE 1:* lorsque le système d'exploitation, le navigateur ou les API de médiation sous-jacents, ou toute autre couche technique échappant au contrôle du portefeuille européen d'identité numérique restreint, filtre, présélectionne ou limite d'une autre manière les formats de justificatifs d'identité, ainsi que les types de PID et d'EAA enregistrés dans le catalogue des de programmes, cette exigence ne peut être satisfaite. Lorsqu'une telle restriction empêche le portefeuille européen d'identité numérique de prendre en charge un type ou un format de justificatif d'identité enregistré, la non-conformité qui en résulte est imputable au fait que ces systèmes d'exploitation, navigateurs, API de médiation ou autres couches techniques pertinentes sous-jacents ne fournissent pas les caractéristiques d'interopérabilité nécessaires.

6) 4.4. Wallet-relying party validation and overasking checks

— WRP-VALIDATION-01: le portefeuille européen d'identité numérique doit valider le certificat d'enregistrement de partie utilisatrice de portefeuille reçu dans la demande avant de présenter toute PID ou attestation électronique d'attributs demandée à l'utilisateur de portefeuille pour approbation.

— WRP-VALIDATION-02: en cas d'échec de la validation du certificat d'enregistrement de partie utilisatrice de portefeuille, y compris lorsque le certificat a expiré, a été révoqué, n'a pas été délivré par un fournisseur de confiance valide de certificats d'enregistrement de partie utilisatrice de portefeuille, n'a pas été correctement formé ou ne peut pas être vérifié par des moyens cryptographiques, le portefeuille européen d'identité numérique doit avertir l'utilisateur de portefeuille que la partie utilisatrice de portefeuille n'a pas pu être validée et ne doit pas indiquer que la validation de la demande a réussi. L'utilisateur de portefeuille doit approuver explicitement la demande de la partie utilisatrice. Ni l'absence de réponse ni des cases cochées par défaut n'ont valeur d'approbation explicite.

— WRP-VALIDATION-03: le fournisseur de portefeuille doit déterminer, sur la base de son analyse des risques et de sa politique de sécurité, si et dans quelles conditions l'utilisateur de portefeuille peut contourner des contrôles de validation spécifiques ayant échoué.

— WRP-OVERASKING-01: le portefeuille européen d'identité numérique doit comparer les attestations et attributs demandés par la partie utilisatrice de portefeuille avec les attestations et attributs enregistrés dans le certificat d'enregistrement de partie utilisatrice de portefeuille.

— WRP-OVERASKING-02: lorsque la partie utilisatrice de portefeuille demande des PID ou des attestations électroniques d'attributs ou des revendications qui ne sont pas couvertes par le certificat d'enregistrement de partie utilisatrice de portefeuille, le portefeuille européen d'identité numérique doit émettre un avertissement clair à l'intention de l'utilisateur de portefeuille avant toute divulgation. L'avertissement doit indiquer que la partie utilisatrice de portefeuille demande davantage d'informations que celles qui ont été enregistrées. L'utilisateur de portefeuille doit approuver explicitement la demande de la partie utilisatrice. Ni l'absence de réponse ni des cases cochées par défaut n'ont valeur d'approbation explicite.

— WRP-OVERASKING-03: le fournisseur de portefeuille doit déterminer, sur la base de son analyse des risques, de sa politique de sécurité et du droit applicable, si l'utilisateur de portefeuille peut continuer malgré cet avertissement, si seul le sous-ensemble de données demandées couvert par le certificat d'enregistrement peut être divulgué ou si la demande doit être rejetée.

7) 5.1. Introduction

— Le paragraphe 5 et ses sous-paragraphes définissent un profil pour un protocole permettant à une RP de demander des EAAP ou des PID au portefeuille européen d'identité numérique, et à ce portefeuille d'envoyer les EAAP/PID demandées à la RP au moyen soit d'un mécanisme de transmission sans médiation d'API, fondé sur la norme ISO/IEC 18013-5 [10], soit d'un mécanisme de transmission avec médiation d'API fondé sur l'annexe C de la norme ISO/IEC 18013-7 [16] pour le transfert des structures de données définies dans la norme ISO/IEC 18013-5 [10] convenablement encapsulées.

— Le reste du paragraphe 5 est organisé comme suit:

  — le paragraphe 5.2 définit les exigences relatives à la prise en charge du profil et des mécanismes de transmission par les RP et le portefeuille européen d'identité numérique;

  — le paragraphe 5.3 précise les exigences spécifiquement applicables au mécanisme de transmission sans médiation d'API;

  — le paragraphe 5.4 et ses sous-paragraphes précisent les exigences spécifiquement applicables au mécanisme de transmission avec médiation d'API.

8) 5.2. Requirements on EUDI Wallet and RP support

— ISO/IEC 18013-SUPPORT-01: les unités de portefeuille, les fournisseurs de PID, les fournisseurs d'attestations, les fournisseurs de portefeuille et les parties utilisatrices ne prennent pas en charge la récupération sur serveur telle que spécifiée dans la norme ISO/IEC 18013-5 [10] pour demander et présenter des PID ou des attributs d'attestations.

— ISO/IEC 18013-SUPPORT-02: le portefeuille européen d'identité numérique doit être conforme aux exigences définies aux paragraphes 5.3 et 5.4 du présent document.

— ISO/IEC 18013-SUPPORT-04: il convient qu'une partie utilisatrice mette en œuvre le profil défini au paragraphe 5.4 du présent document.

9) 5.3.2 ISO/IEC-mdoc EAAP Request contents

— ISO/IEC 18013-5-REQ-04: les demandes envoyées par l'appareil au portefeuille européen d'identité numérique doivent contenir la paire clé-valeur 'requestInfo' spécifiée au paragraphe 8.3.2.1.2.1 de [10]. La valeur de cette paire doit être du type RequestInfo.

— ISO/IEC 18013-5-REQ-05: le type RequestInfo doit correspondre à la définition CDDL ci-dessous:

```
RequestInfo = {

    'euWrprc': bstr ; contient un certificat d'enregistrement (voir les exigences ci-dessous)

}
```

— ISO/IEC 18013-5-REQ-06: le membre requestInfo mentionné doit comporter un membre muni de l'étiquette 'euWrprc'.

— ISO/IEC 18013-5-REQ-07: la valeur de la paire 'euWrprc' doit être un certificat d'enregistrement encodé au format CBOR.

— ISO/IEC 18013-5-REQ-08: vide.

— *REMARQUE 3:* vide.

— ISO/IEC 18013-5-REQ-09: vide.

— ISO/IEC 18013-5-REQ-10: vide.

— ISO/IEC 18013-5-REQ-11: vide.

10) 5.3.3. ISO/IEC-mdoc EAAP Response profile

— Le présent paragraphe définit les exigences applicables au type de message DeviceResponse, commun aux deux types de mécanismes de transmission (avec et sans médiation d'API).

— *REMARQUE 1:* lorsqu'un mécanisme sans médiation d'API fondé sur la norme ISO/IEC 18013-5 [10] est utilisé, une réponse EAAP est exactement une instance de DeviceResponse telle que décrite dans le présent paragraphe. Lorsqu'un mécanisme avec médiation d'API fondé sur l'annexe C de la norme ISO/IEC 18013-7 [16] est utilisé, l'instance de DeviceRequest est encapsulée comme spécifié à l'annexe C du [16].

— ISO/IEC 18013-5-RESP-02: le fournisseur de données d'identification personnelle et d'attestations électroniques d'attributs n'inclut aucun élément de données de la table associative KeyAuthorizations de l'objet de sécurité mobile des données d'identification personnelle et des attestations électroniques d'attributs qu'il délivre, à l'exception des éléments de données qui sont fournis par la partie utilisatrice de portefeuille dans les données transactionnelles de la demande mdoc, qui doit être signée ou cachetée par l'unité de portefeuille à l'aide de la clé privée des données d'identification personnelle ou des attestations électroniques d'attributs.

— *REMARQUE 2:* par conséquent, les unités de portefeuille ne peuvent pas présenter aux parties utilisatrices de portefeuille d'éléments de données signés par le dispositif, à l'exception des données que la partie utilisatrice de portefeuille a fournies, par exemple pour une authentification sécurisée de l'utilisateur.

— *REMARQUE 3:* la norme ISO/IEC 18013-5: 2021 ne précise pas comment les parties utilisatrices de portefeuille peuvent inclure des données transactionnelles dans une demande mdoc. L'inclusion de données transactionnelles dans une demande mdoc nécessite des spécifications techniques supplémentaires.

— ISO/IEC 18013-5-RESP-03: les fournisseurs de données d'identification personnelle n'autorisent pas la clé privée des données d'identification personnelle à signer les éléments de données qui sont fournis par la partie utilisatrice de portefeuille dans les données transactionnelles figurant dans la demande mdoc.

11) 5.4. Requirements for API mediated mechanism

5.4.1. ISO/IEC 18013-7-related requirements

Le présent paragraphe définit les exigences applicables au mécanisme de transmission avec médiation d'API en rapport avec les exigences définies à l'annexe C du [16].

— ISO/IEC 18013-7-API-01: le profil prenant en charge les présentations avec médiation d'API doit être conforme aux exigences de l'annexe C de la norme ISO/IEC 18013-7 [16] telles que précisées dans les paragraphes 5.3 et 5.4 du présent document.

— ISO/IEC 18013-7-API-02: toutes les exigences obligatoires définies à l'annexe C du [16] sont applicables, telles que précisées dans les paragraphes 5.3 et 5.4 du présent document.

— ISO/IEC 18013-7-API-03: toutes les exigences facultatives définies à l'annexe C du [16] doivent rester facultatives, sauf indication contraire dans le présent document.

12) 5.4.2. Additional requirements

— Le présent paragraphe spécifie des exigences supplémentaires pour le mécanisme de transmission avec médiation d'API.

— ISO/IEC 18013-ADD-API-01: le portefeuille européen d'identité numérique doit divulguer par défaut la présence de tous les types d'attestations électroniques d'attributs stockés à l'API de médiation qui fonctionne conformément à l'annexe C du [16], mais il ne doit pas divulguer les attributs et leurs valeurs dans ces attestations électroniques d'attributs.

— *REMARQUE 1:* la restriction concernant la valeur des attributs s'applique même si cette divulgation aurait pour effet d'améliorer les services fournis par le système d'exploitation au portefeuille, par exemple la sélection de l'attestation dans le cadre de l'API assurant la médiation.

— Certaines considérations relatives aux systèmes d'exploitation et aux navigateurs échappent au contrôle des responsables de la mise en œuvre et peuvent être prises en compte comme indiqué dans les remarques 2 à 4 suivantes:

— *REMARQUE 2:* une demande de présentation émanant d'une partie utilisatrice prenant en charge l'annexe C du [16] peut être traitée par le navigateur et/ou le système d'exploitation pour rechercher des EAA disponibles, pour prévenir une fraude ciblant l'utilisateur ou à des fins de dépannage.

— *REMARQUE 3:* une demande de présentation émanant d'une partie utilisatrice prenant en charge l'annexe C du [16] est censée être traitée par le navigateur et/ou le système d'exploitation pour la sécurité de l'utilisateur.

— *REMARQUE 4:* une demande de présentation émanant d'une partie utilisatrice prenant en charge l'annexe C de [16] ne devrait pas être traitée par le navigateur et/ou le système d'exploitation à des fins d'analyse de marché (y compris à titre secondaire) ou à des fins internes du navigateur et/ou du système d'exploitation.

— ISO/IEC 18013-ADD-API-02: lorsqu'un portefeuille européen d'identité numérique supprime, à la demande de l'utilisateur, des PID ou une EAA précédemment divulguées à l'API assurant la médiation qui fonctionne conformément à l'annexe C du [16], le portefeuille indique à l'API assurant la médiation qu'il ne stocke plus ces PID ou cette EAA.

— ISO/IEC 18013-ADD-API-03: si l'utilisateur désinstalle son portefeuille européen d'identité numérique, le portefeuille divulgue le fait qu'il ne stocke plus aucun des PID ou EAA précédemment divulgués à l'API de médiation qui fonctionne conformément à l'annexe C du [16].

— ISO/IEC 18013-ADD-API-04: le portefeuille européen d'identité numérique comporte un paramètre utilisateur global permettant de désactiver la divulgation des EAA stockées via une API de médiation qui fonctionne conformément aux spécifications de la norme ISO/IEC 18013-ADD-API-01. Lorsque ce paramètre est désactivé, le portefeuille ne fait pas d'annonce ou ne répond pas aux demandes de présentation ou d'émission transmises par l'API.

— ISO/IEC 18013-ADD-API-05: les portefeuilles européens d'identité numérique vérifient dans les flux multi-appareils, à l'aide de l'API de médiation, que l'appareil qui interagit se trouve à proximité physique immédiate du portefeuille européen d'identité numérique, au moyen d'un canal de communication local sécurisé, direct et nécessitant une action de l'utilisateur, tel qu'une technologie de communication sans fil à courte portée, pour effectuer la vérification de proximité physique.

— *REMARQUE:* le protocole CTAP 2.3 permet d'utiliser le BLE pour effectuer la vérification de proximité physique immédiate et, lorsqu'il est mis en œuvre par les deux appareils, permet également de transporter les données d'un appareil à l'autre au moyen de technologies de transmission à courte portée. Les systèmes d'exploitation, navigateurs, API de médiation sous-jacents ou toute autre couche technique échappant au contrôle du portefeuille européen d'identité numérique devraient utiliser, pour réaliser tant la vérification de proximité physique que le transfert de données entre les deux appareils, un canal de communication local comme prévu par le CTAP 2.3 plutôt que de recourir aux services de transport hybride CTAP.

13) 6.2 Requirements on EUDI Wallet and RP support

— OIDFVP-HAIP-SUPPORT-02: le portefeuille européen d'identité numérique doit être conforme aux exigences définies au paragraphe 6.5 de la présente annexe.

— OIDFVP-HAIP-SUPPORT-03: le portefeuille européen d'identité numérique ne devrait pas prendre en charge le mécanisme fondé sur les redirections spécifié au paragraphe 6.4 pour les flux de présentation multi-appareils.

— *REMARQUE 3:* ce mécanisme est vulnérable aux attaques, notamment par fixation des sessions. Il appartient aux parties utilisatrices d'atténuer ces attaques. La mise en œuvre de ce mécanisme ne devrait pas entraîner de non-conformité.

— OIDFVP-HAIP-SUPPORT-05: une partie utilisatrice doit être conforme aux exigences définies au paragraphe 6.5 de la présente annexe.

— *REMARQUE 5:* vide.

14) 6.3.1. General requirements

— OIDFVP-HAIP-GEN-01: toutes les exigences obligatoires énoncées aux paragraphes 5, 5.3, 7 et 8 de HAIP [11] s'appliquent.

— *REMARQUE 1:* "Section 5 de HAIP [11]" renvoie uniquement aux exigences énoncées directement sous l'intitulé "Section 5". Cela n'inclut pas les sections 5.1, 5.2 et 5.3.

— OIDFVP-HAIP-GEN-03: si la présente annexe modifie une exigence dans OpenID4VC-HAIP [11], l'exigence modifiée spécifiée par la présente annexe prévaut.

— *REMARQUE 2:* cela permettrait, par exemple, de rendre obligatoire une exigence facultative de OpenID4VC-HAIP [11] ou d'étendre des exigences obligatoires.

— OIDFVP-HAIP-GEN-04: lorsque le format de l'attestation demandée est conforme à [10], les parties utilisatrices et les portefeuilles européens d'identité numérique doivent être conformes au profil 'ISO mdocs' figurant à la section 6 de [11].

— *REMARQUE 3:* éclaircissement: le profil 'ISO mdocs' dans HAIP implique que les parties utilisatrices et les portefeuilles européens d'identité numérique doivent être conformes aux exigences applicables figurant à la section [7] de l'annexe B.2.

— OIDFVP-HAIP-GEN-05: lorsque le format de l'attestation demandée est conforme à [2], les parties utilisatrices et les portefeuilles européens d'identité numérique doivent être conformes au profil 'IETF SD-JWT VCs' figurant à la section 6 de [11].

— *REMARQUE 4:* éclaircissement: le profil 'IETF SD-JWT VCs' implique que les parties utilisatrices et les portefeuilles européens d'identité numérique doivent être conformes aux exigences figurant à la section [7] de l'annexe B.3, ainsi qu'aux exigences figurant à la section 6.1 de [11].

15) 6.3.2.1 General requirements

— OIDFVP-HAIP-COMMON-REQ-01: vide.

16) 6.3.2.2 Requirements for the Request Object

— OIDFVP-HAIP-COMMON-REQ-RO-02: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-03: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-04: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-05: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-06: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-07: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-08: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-09: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-10: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-11: vide.

— OIDFVP-HAIP-COMMON-REQ-RO-12: vide.

— *Remarque 2:* vide.

— OIDFVP-HAIP-COMMON-REQ-RO-13: l'un des éléments du paramètre verifier_info comprend le certificat d'enregistrement.

— OIDFVP-HAIP-COMMON-REQ-RO-23: le certificat d'entité finale mentionné dans la section 5.9.3 d'OpenID4VP, à utiliser avec le x509_hash Client Identifier Prefix est un certificat d'accès de RP tel que spécifié dans ETSI TS 119 475 [14].

17) 6.3.3 Authorization Response (EAAP response) profile

— OIDFVP-HAIP-COMMON-RESP-01: vide.

18) 6.4.1 General requirements

— OIDFVP-HAIP-REDIRECTS-04: vide.

— *REMARQUE:* vide.

19) 6.5.2 General requirements

— OIDFVP-HAIP-ADD-API-01: le portefeuille européen d'identité numérique doit divulguer par défaut la présence de tous les types d'EAA stockées à l'API assurant la médiation qui fonctionne conformément au paragraphe 5.2 de [11], mais il ne doit pas divulguer les attributs et leurs valeurs dans ces EAA.

— OIDFVP-HAIP-ADD-API-04: si le portefeuille européen d'identité numérique prend en charge une API de médiation qui fonctionne comme indiqué dans OIDFVP-HAIP-ADD-API-01, il doit comporter un paramètre utilisateur global permettant de désactiver la divulgation des EAA stockées par l'intermédiaire de l'API de médiation. Lorsque ce paramètre est configuré en divulgation désactivée, le portefeuille européen d'identité numérique devrait ensuite permettre à l'utilisateur de sélectionner individuellement les attestations à divulguer à l'API de médiation.

— OIDFVP-HAIP-ADD-API-05: les portefeuilles européens d'identité numérique doivent utiliser, dans les flux multi-appareils, l'API de médiation pour vérifier que l'appareil qui interagit se trouve à proximité physique immédiate du portefeuille européen d'identité numérique, au moyen d'un canal de communication local sécurisé, direct et nécessitant une action de l'utilisateur, tel qu'une technologie de communication sans fil à courte portée, pour effectuer la vérification de proximité physique.

— *REMARQUE 5:* le protocole CTAP 2.3 permet d'utiliser le BLE pour effectuer la vérification de proximité physique immédiate et, lorsqu'il est mis en œuvre par les deux appareils, permet également de transporter les données d'un appareil à l'autre au moyen de technologies de transmission à courte portée. Les systèmes d'exploitation, navigateurs, API de médiation sous-jacents ou toute autre couche technique échappant au contrôle du portefeuille européen d'identité numérique devraient utiliser, pour réaliser tant la vérification de proximité physique que le transfert de données entre les deux appareils, un canal de communication local comme prévu par le CTAP 2.3 plutôt que de recourir aux services de transport hybride CTAP.

20) 6.5.3 Specific requirements when requesting ISO/IEC 18013-5 EAAP

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: toutes les exigences énoncées dans le présent document applicables aux structures Device Request et Device Response précisées dans ISO/IEC 18013-5 sont également applicables lorsque le portefeuille européen d'identité numérique reçoit une demande de présentation ISO/IEC mdoc via un mécanisme transmis par API figurant dans le paragraphe C.1 de [16].»

Journal officiel
de l'Union européenne

FR
Série L

2026/1735

22.7.2026

RÈGLEMENT D'EXÉCUTION (UE) 2026/1735 DE LA COMMISSION

du 15 juillet 2026

modifiant le règlement d'exécution (UE) 2025/1569 en ce qui concerne les normes et spécifications applicables

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) n° 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 *quinquies*, paragraphe 5, son article 45 *sexies*, paragraphe 2, et son article 45 *septies*, paragraphes 6 et 7,

considérant ce qui suit:

(1) Afin de garantir le niveau d'harmonisation le plus élevé possible entre les États membres en matière de développement des portefeuilles européens d'identité numérique, les spécifications techniques applicables aux portefeuilles s'appuient sur les travaux réalisés sur la base de la recommandation (UE) 2021/946 de la Commission ([2]) et, en particulier, sur l'architecture et le cadre de référence. Étant donné que l'architecture et le cadre de référence ont considérablement évolué depuis l'adoption du règlement d'exécution (UE) 2025/1569 de la Commission ([3]), il convient à présent de modifier ledit règlement d'exécution afin de l'aligner sur les nouvelles normes et spécifications.

(2) Conformément aux objectifs du règlement (UE) n° 910/2014, un certain nombre de normes ont été sélectionnées pour satisfaire aux exigences applicables en matière de délivrance, de gestion et de vérification des attestations électroniques d'attributs. Ces normes devraient tenir compte des pratiques établies et être largement reconnues dans les secteurs concernés. Si nécessaire, ces normes devraient être adaptées ou complétées afin de garantir un niveau élevé de sécurité et d'intégrité des attestations électroniques d'attributs, tout en facilitant l'interopérabilité transfrontière et le bon fonctionnement du marché intérieur. Conformément à cet objectif, le présent règlement met à jour les exigences applicables à la délivrance et à la révocation des attestations électroniques d'attributs qualifiées et des attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte et introduit les exigences relatives à l'apposition d'une signature et d'un cachet sur les résultats de vérification par rapport aux sources authentiques.

(3) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([4]) et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([5]) 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]) Recommandation (UE) 2021/946 de la Commission du 3 juin 2021 concernant une boîte à outils commune de l'Union pour une approche coordonnée en vue d'un cadre européen relatif à une identité numérique (JO L 210 du 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reg/2021/946/oj).

([3]) Règlement d'exécution (UE) 2025/1569 de la Commission du 29 juillet 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les attestations électroniques d'attributs qualifiées et les attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte (JO L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([4]) 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).

([5]) 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).

(4) 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 17 avril 2026 ([7]).

(5) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Modification du règlement d'exécution (UE) 2025/1569

Le règlement d'exécution (UE) 2025/1569 est modifié comme suit:

1) À l'article 3, le paragraphe 2 est remplacé par le texte suivant:

«2. Lorsque les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte délivrent des attestations électroniques d'attributs qui sont couvertes par des programmes enregistrés dans le catalogue de programmes d'attestation d'attributs, ils se conforment aux exigences du programme d'attestation d'attributs correspondant. Les règles et procédures établies par les entités délivrant des attestations pour satisfaire aux exigences des programmes d'attestation d'attributs sont prises en compte dans l'évaluation de la conformité prévue par le règlement (UE) nº 910/2014.».

2) L'article 4 est modifié comme suit:

a) le paragraphe 1 est supprimé;

b) le paragraphe 3 est remplacé par le texte suivant:

«3. Lorsque la période de validité des attestations fournies par les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte est supérieure à 24 heures, les fournisseurs de ces attestations les révoquent au moins dans les cas suivants:

a) à la demande de la personne à laquelle l'attestation électronique d'attributs a été délivrée ou, le cas échéant, de la personne à laquelle l'attestation se rapporte;

b) lorsque le fournisseur apprend que la sécurité ou la fiabilité des attestations électroniques d'attributs qualifiées ou des attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte a été compromise;

c) dans d'autres situations, comme le requiert la législation de l'Union ou le droit national.»;

c) le paragraphe 4 est remplacé par le texte suivant:

«4. Les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte mettent en place des techniques de révocation et des méthodes de gestion des révocations qui garantissent la protection de la vie privée et empêchent l'associabilité et la traçabilité. Les techniques de révocation satisfont aux exigences énoncées à l'annexe II.».

([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) nº 45/2001 et la décision nº 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 Commission Implementing Regulation as regards applicable standards and specifications for the registration of wallet-relying parties | (Commentaires formels du CEPD sur le projet de règlement d'exécution de la Commission en ce qui concerne les normes et spécifications applicables pour l'enregistrement des parties utilisatrices de portefeuille)Contrôleur européen de la protection des données.

3) L'article 9 est modifié comme suit:

a) le paragraphe 2 *bis* suivant est inséré après le paragraphe 2:

«2 *bis* Le mécanisme de vérification satisfait aux spécifications énoncées à l'annexe IV.»;

b) le paragraphe 4 est remplacé par le texte suivant:

«4. Le résultat de la vérification indique si l'attribut a été vérifié ou non et précise l'organisme du secteur public responsable de la source authentique ou, le cas échéant, l'organisme du secteur public désigné pour agir pour le compte de la source authentique ayant servi à la vérification de l'attribut.

Le résultat de la vérification est signé ou cacheté par l'organisme du secteur public responsable d'une source authentique, ou par l'intermédiaire désigné reconnu au niveau national, au moyen, au moins, d'une signature électronique avancée reposant sur un certificat qualifié de signature électronique ou d'un cachet électronique avancé reposant sur un certificat qualifié de cachet électronique, respectivement.».

4) L'annexe I est remplacée par le texte figurant à l'annexe I du présent règlement.

5) L'annexe II est remplacée par le texte figurant à l'annexe II du présent règlement.

6) Le texte figurant à l'annexe III du présent règlement est ajouté en tant qu'annexe IV.

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*.

L'article 1er, paragraphe 3, est applicable à partir du 1er janvier 2027.

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

Fait à Bruxelles, le 15 juillet 2026.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE I

«*ANNEXE I*

Liste des normes de référence et des spécifications mentionnées à l'article 3

ETSI TS 119 471 V1.1.1 (2025-05) s'applique, moyennant les adaptations suivantes:

1) 2.1 Références normatives

[1] ETSI EN 319 401 V3.2.1 (2026-01): "Signatures électroniques et infrastructures de confiance; exigences de politique générale applicables des prestataires de services de confiance";

[2] 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] FIPS PUB 140-3 (2019) "Security Requirements for Cryptographic Modules";

[4] Règlement d'exécution (UE) 2024/482 de la Commission ([1]);

[5] Règlement d'exécution (UE) 2024/3144 de la Commission ([2]);

[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".

2) 3.1 Termes

Le terme suivant est ajouté:

— 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.

3) 4. Services de confiance de l'EAA

— La clause 4.2.2.2 «Vérification des attributs par rapport aux sources authentiques» ne s'applique pas.

— REQ-EAASP-4.2.2.3-02: Le prestataire de services d'attestation électronique d'attribut s'authentifie auprès de l'instance d'EUDIW en mettant en œuvre des mécanismes d'authentification mutuelle qui utilisent un certificat d'accès valide.

— REQ-EAASP-4.2.2.3-03: Le prestataire de services d'attestation électronique d'attribut valide l'unité d'EUDIW et vérifie si l'instance d'EUDIW est révoquée.

— La clause *4.3.2 'EUDIW Specific' ne s'applique pas.*

4) 6.1 Énoncé de pratique de l'EAAS:

— REQ-EAASP-6.1-02: Le prestataire de services d'attestation électronique d'attribut (EAASP) expose le mécanisme de révocation dans l'énoncé de pratique du service d'attestation électronique d'attribut (EAAS).

5) 6.3 Politique en matière de sécurité de l'information:

— REQ-EAASP-6.3-02: Le prestataire de services d'attestation électronique d'attribut établit des procédures pour informer l'organe de contrôle de toute modification apportée à la fourniture du service de confiance pour l'attestation électronique d'attributs et de l'intention de cesser ces activités, conformément aux exigences opérationnelles et aux dispositions législatives et réglementaires applicables, y compris conformément aux exigences des actes d'exécution adoptés en vertu de l'article 24, paragraphe 5, du règlement (UE) n° 910/2014. Le prestataire de services d'attestation électronique d'attribut 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.

([1]) 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/oj).

([2]) 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).

6) 7.5 Contrôles cryptographiques

— REQ-EAASP-7.5.2-05: néant

— REQ-EAASP-7.5.2-06: néant

— REQ-EAASP-7.5.3-01A: 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-EAASP-7.5.3-01B: Aux fins de la fourniture de ses services de confiance, le prestataire de services d'attestation électronique d'attribut 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 [2].

— REQ-EAASP-7.5.3-02: Le prestataire de services d'attestation électronique d'attribut veille à ce que le dispositif cryptographique sécurisé qu'il utilise pour la signature ou le cachet numérique de l'attestation électronique d'attribut soit un dispositif de création de signature ou de cachet qualifié et à ce que tous les autres signatures ou cachets numériques utilisés pour fournir le service de confiance pour l'attestation électronique d'attributs correspondant, ou une partie de celui-ci, soient créés au moyen d'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 les critères communs pour l'évaluation de la sécurité des technologies de l'information, version 3.1 (CC3.1) jusqu'au 31.8.2027, ou dans la 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, ou dans la norme ISO/IEC 15408 [6], et certifiés au niveau EAL 4 ou supérieur; ou

  (b) au schéma européen commun de certification de cybersécurité fondé sur des critères communs (EUCC) [4][5] et certifié au niveau EAL 4 ou supérieur; ou

  (c) à la norme FIPS-140-2 niveau 3 à utiliser jusqu'au 31.8.2027 pour les systèmes certifiés existants ou à la norme FIPS PUB 140-3 [3] niveau 3 jusqu'au 31.12.2030.

  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 doit être configuré et utilisé conformément à cette certification.

— REQ-EAASP-7.5.5-01: néant

— REQ-EAASP-7.5.5-02: néant

— REQ-EAASP-7.5.5-04: néant

7) 7.9 Vulnérabilités et gestion des incidents

— REQ-EAASP-7.9-02: Les activités de surveillance tiennent compte de la sensibilité de toute information collectée ou analysée.

8) 7.12 Cessation d'activité et plans de cessation de l'EAASP et de l'EAAS:

— REQ-EAASP-7.12-04: Le plan de cessation d'activité du prestataire de services d'attestation électronique d'attribut 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].».

ANNEXE II

«*ANNEXE II*

Spécifications techniques visées à l'article 3 et à l'article 4

Les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte délivrent leurs attestations conformément à l'une au moins des normes énumérées à l'annexe II du règlement d'exécution (UE) 2024/2979 de la Commission ([1]) et appliquent les techniques de révocation correspondantes, également énoncées dans l'annexe II du règlement d'exécution (UE) 2024/2979 de la Commission.».

([1]) Règlement d'exécution (UE) 2024/2979 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne l'intégrité et les fonctionnalités essentielles des portefeuilles européens d'identité numérique (JO L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

ANNEXE III

«ANNEXE IV

Liste des normes et des spécifications techniques mentionnées à l'article 9

Les mécanismes de vérification visés à l'article 9 sont conformes à l'un des éléments suivants, ou aux deux, moyennant les adaptations suivantes:

a) les spécifications techniques énoncées dans la clause 6.1.1 de la norme ETSI TS 119 478 V1.1.1 (2026-01) - Signatures électroniques et infrastructures de confiance (ESI); Spécification des interfaces liées aux sources authentiques;

— REQ-ASIP-6.1.1.2-04-01 [CONDITIONNEL]: Dans le cas où attributeVerificationResult est soit http://uri.etsi.org/19478/VerificationResult/Match soit http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, attributeVerificationResult peut contenir un élément attributeValue.

— REQ-ASIP-6.1.1.2-04-02 [CONDITIONNEL]: Dans le cas où attributeVerificationResult renvoyé est http://uri.etsi.org/19478/VerificationResult/Match et où attributeVerificationResult contient un élément attributeValue, l'élément attributeValue doit contenir la valeur indiquée dans la demande.

— REQ-ASIP-6.1.1.2-04-03 [CONDITIONNEL]: Dans le cas où attributeVerificationResult renvoyé est http://uri.etsi.org/19478/VerificationResult/MatchWithVariation et où attributeVerificationResult contient un élément attributeValue, l'élément attributeValue doit contenir la valeur de l'attribut telle que stockée dans la source authentique.

— REQ-ASIP-6.1.1.2-06-04-01 [CONDITIONNEL]: Dans le cas où fragmentVerificationResult est soit http://uri.etsi.org/19478/VerificationResult/Match soit http://uri.etsi.org/19478/VerificationResult/MatchWithVariation attributeVerificationResult peut contenir un élément fragmentValue.

— REQ-ASIP-6.1.1.2-06-04-02 [CONDITIONNEL]: Dans le cas où fragmentVerificationResult renvoyé est http://uri.etsi.org/19478/VerificationResult/Match et où attributeVerificationResult contient un élément fragmentValue, l'élément fragmentValue doit contenir la valeur indiquée dans la demande.

— REQ-ASIP-6.1.1.2-06-04-03 [CONDITIONNEL]: Dans le cas où fragmentVerificationResult renvoyé est http://uri.etsi.org/19478/VerificationResult/MatchWithVariation et où attributeVerificationResult contient un élément fragmentValue, l'élément fragmentValue doit contenir la valeur du fragment de l'attribut telle que stockée dans la source authentique.

b) les spécifications techniques énoncées dans la clause 6.2.3 de la norme ETSI TS 119 478 V1.1.1 (2026-01) - Signatures électroniques et infrastructures de confiance (ESI); Spécification des interfaces liées aux sources authentiques.

— REQ-ASIP-6.2.3.2.1-08-04: L'élement AttributeVerificationResponse peut contenir exactement un élément enfant au choix entre TextValue, XMLValue ou AttributeProperties.».

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].

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.

Journal officiel
de l'Union européenne

FR
Série L

2025/1568

30.7.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/1568 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 modalités de procédure pour les examens par les pairs des schémas d'identification électronique et pour la coopération relative à l'organisation de ces examens au sein du groupe de coopération, et abrogeant la décision d'exécution (UE) 2015/296 de la Commission

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 12, paragraphe 6, et son article 46 *sexies*, paragraphe 7,

considérant ce qui suit:

(1) Le règlement (UE) nº 910/2014 prévoit un mécanisme d'examen par les pairs en ce qui concerne les schémas d'identification électronique qui doivent être notifiés, auquel les États membres peuvent participer sur une base volontaire. Les examens par les pairs devraient permettre aux États membres de comprendre les schémas d'identification électronique qui doivent être notifiés en application de l'article 9, paragraphe 1, point a), du règlement (UE) nº 910/2014 et de coopérer efficacement en vue d'assurer l'interopérabilité de ces schémas et de renforcer la confiance dans l'ensemble de l'Union. Les examens par les pairs devraient être organisés de manière à garantir une répartition équitable des efforts et une large représentation de tous les États membres et ne devraient pas être considérés comme des audits.

(2) La décision d'exécution (UE) 2015/296 de la Commission ([2]) a établi les modalités de procédure applicables à la coopération relative aux schémas d'identification électronique dans le contexte de l'ancien réseau de coopération eIDAS, y compris en ce qui concerne les examens par les pairs réalisés par les membres de ce réseau. Dès lors que l'organisation des tâches d'examen par les pairs relève désormais du groupe de coopération européen en matière d'identité numérique établi, comme prévu par l'article 46 *sexies*, paragraphe 1, du règlement (UE) nº 910/2014, par la décision C(2024) 6132 de la Commission du 5.9.2024 établissant le groupe de coopération européen en matière d'identité numérique et modifiant la décision d'exécution (UE) 2015/296 (ci-après le «groupe de coopération»), il convient d'abroger la décision d'exécution (UE) 2015/296.

(3) Dans un souci d'accessibilité des examens par les pairs, tout État membre devrait pouvoir en demander le déclenchement. La demande devrait mentionner les raisons pour lesquelles l'examen par les pairs est sollicité et contenir suffisamment d'informations pour confirmer que ce dernier peut contribuer à l'interopérabilité ou à la sécurité des schémas d'identification électronique devant être notifiés. À cette fin, il est nécessaire de créer des règles uniformes en ce qui concerne les informations minimales requises pour que l'examen par les pairs puisse être mené à bien avec efficience et en temps utile. La Commission peut organiser des réunions du groupe de coopération afin de faciliter le déclenchement et la conclusion en temps utile d'un examen par les pairs.

(4) Lorsqu'un État membre fournit aux autres États membres des informations sur un schéma d'identification électronique en application de l'article 7, point g), du règlement (UE) nº 910/2014 («notification préalable»), cette mesure devrait être formellement considérée comme une demande de l'État membre notifiant de procéder à un examen par les pairs de son schéma d'identification électronique.

([1]) JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/ojhttp://data.europa.eu/eli/reg/2014/910/2024-10-18.

([2]) Décision d'exécution (UE) 2015/296 de la Commission du 24 février 2015 établissant les modalités de coopération entre les États membres en matière d'identification électronique conformément à l'article 12, paragraphe 7, du règlement (UE) nº 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (JO L 53 du 25.2.2015, p. 14, ELI: http://data.europa.eu/eli/dec_impl/2015/296/oj).

(5) Pour assurer une préparation et une exécution efficaces de l'examen par les pairs, il convient d'y définir des rôles et des responsabilités normalisés. Les États membres devraient avoir la possibilité de désigner des représentants pour exercer ces rôles et responsabilités. Comme il est essentiel que tous les examens par les pairs se déroulent avec fluidité et s'effectuent de manière rationalisée et rapide, il convient que les modalités pratiques de chaque examen par les pairs, telles que, à titre indicatif, sa portée exacte et son calendrier, soient arrêtées d'un commun accord entre les États membres y participant.

(6) Afin que tous les États membres contribuent à la mise en œuvre du mécanisme d'examen par les pairs et puissent tirer profit de l'apprentissage entre pairs, les représentants de chaque État membre devraient contribuer à une répartition équitable des efforts entre les États membres pour tous les examens par les pairs à réaliser.

(7) Afin de favoriser un niveau de confiance élevé dans les schémas d'identification électronique faisant l'objet d'une évaluation par les pairs, les États membres devraient fournir les informations minimales requises, tout en garantissant la confidentialité des informations potentiellement sensibles. Ces informations devraient être évaluées par trois groupes de travail dans le cadre des examens par les pairs, ayant chacun un mandat correspondant aux éléments déterminants pour l'évaluation d'un schéma d'identification électronique conformément au règlement d'exécution (UE) 2015/1501 de la Commission ([3]) et au règlement d'exécution (UE) 2015/1502 de la Commission ([4]).

(8) La décision d'exécution (UE) 2015/296 ayant déjà désigné l'anglais comme langue de coopération, à moins qu'il n'en soit convenu autrement, la pratique existante veut que les États membres procèdent à l'examen par les pairs en anglais. Par conséquent, les États membres devraient fournir au moins en anglais les informations pertinentes pour l'examen par les pairs. Toutefois, la traduction ne devrait pas entraîner de charges administratives ou financières déraisonnables. Dans ces conditions, il est loisible aux États membres d'utiliser des outils de traduction automatique, y compris ceux fournis par la Commission.

(9) Compte tenu de l'importance des examens par les pairs en tant qu'outil permettant de garantir la fiabilité des schémas d'identification électronique notifiés, il convient de mettre en place un processus rationalisé pour l'adoption d'un rapport final d'examen par les pairs à la fois clair et complet. Au cours de ce processus, le groupe de coopération et les États membres participant à l'examen par les pairs devraient avoir la possibilité de poser des questions supplémentaires à l'État membre dont le schéma d'identification électronique fait l'objet de l'examen par les pairs, tandis que ledit État membre devrait avoir la possibilité de formuler des observations supplémentaires. Dans un souci de transparence, le processus devrait s'achever par la publication de l'avis du groupe de coopération sur la conclusion de l'examen par les pairs.

(10) Étant donné que les schémas d'identification électronique peuvent subir des modifications après la conclusion de leur examen par les pairs, il est également nécessaire de mettre en place un processus permettant de déclencher une actualisation des examens par les pairs réalisés antérieurement si ces modifications peuvent avoir une incidence sur l'interopérabilité, la sécurité ou la fiabilité du schéma d'identification électronique notifié. Cela permettrait de préserver la pertinence des examens par les pairs dans le temps à mesure que les schémas d'identification électronique évoluent.

(11) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([5]) ainsi que, le cas échéant, le règlement (UE) 2018/1725 du Parlement européen et du Conseil ([6]) et la directive 2002/58/CE du Parlement européen et du Conseil ([7]) s'appliquent aux activités de traitement de données à caractère personnel au titre du présent règlement.

([3]) Règlement d'exécution (UE) 2015/1501 de la Commission du 8 septembre 2015 sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (JO L 235 du 9.9.2015, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2015/1501/oj).

([4]) Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (JO L 235 du 9.9.2015, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([5]) 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).

([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]) 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).

(12) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 et a rendu son avis le 28 mai 2025.

(13) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Principes généraux de l'examen par les pairs

1. Lorsqu'un État membre procède à la notification préalable d'un schéma d'identification électronique à la Commission et aux autres États membres, l'examen par les pairs est déclenché conformément à l'article 2.

2. L'État membre qui procède à la notification préalable d'un schéma d'identification électronique peut, à tout moment, retirer sa notification préalable. Lorsque l'État membre retire sa notification préalable du schéma d'identification électronique, l'examen par les pairs est considéré comme ayant pris fin.

3. Tout État membre peut décider de participer à l'examen par les pairs du schéma d'identification électronique d'un autre État membre.

4. Chaque État membre prenant part à un examen par les pairs supporte les coûts qu'il effectue dans le cadre de sa participation au processus.

5. Les représentants des États membres qui procèdent à l'examen par les pairs utilisent les informations obtenues dans le cadre de l'examen par les pairs aux seules fins de cet examen et ne divulguent à des tiers aucune information sensible ou confidentielle obtenue au cours de l'examen par les pairs.

6. Un État membre qui décide de participer à l'examen par les pairs d'un schéma d'identification électronique d'un autre État membre divulgue tout conflit d'intérêts concernant les représentants désignés par cet État membre. En cas de conflit d'intérêts, l'État membre dont le schéma d'identification électronique fait l'objet de l'évaluation par les pairs peut refuser la participation du représentant concerné à l'évaluation de son schéma d'identification électronique.

7. Tout différend survenant au cours de l'examen par les pairs en ce qui concerne les activités d'examen par les pairs prévues à l'article 4, paragraphe 4, du présent règlement est réglé conformément au règlement intérieur du groupe de coopération.

8. Un schéma d'identification électronique n'est pas soumis à un nouvel examen par les pairs dans les deux ans suivant la conclusion d'un examen par les pairs, sauf si des modifications importantes au sens de l'article 6, paragraphe 1, ont été apportées au schéma d'identification électronique ayant fait l'objet de l'examen par les pairs.

Article 2

Déclenchement de l'examen par les pairs

1. La notification préalable comprend au minimum:

a) une comparaison entre le schéma d'identification électronique faisant l'objet de la notification préalable et les exigences énoncées dans le règlement d'exécution (UE) 2015/1502, sous la forme d'une table de correspondance des niveaux de garantie pour l'examen par les pairs conformément à l'annexe I du présent règlement;

b) une description générale du schéma d'identification électronique, de son écosystème et de l'identification électronique dans l'État membre ayant procédé à la notification préalable, sous la forme d'un livre blanc conformément à l'annexe II du présent règlement;

c) des informations concernant l'interopérabilité du schéma d'identification électronique par rapport aux exigences énoncées dans le règlement d'exécution (UE) 2015/1501, sous la forme d'une table de correspondance du cadre d'interopérabilité conformément au modèle figurant à l'annexe III du présent règlement.

2. La Commission diffuse les informations de la notification préalable au groupe de coopération.

3. Les informations requises en vertu du paragraphe 1, point c), sont fournies au moins en anglais. Les États membres ne sont pas tenus de faire traduire les documents si cela engendre une charge administrative ou financière déraisonnable.

Article 3

Préparation de l'examen par les pairs

1. Dès confirmation de la réception d'une notification préalable complète, la Commission informe le groupe de coopération du déclenchement de l'examen par les pairs et programme une réunion en inscrivant à l'ordre du jour le schéma d'identification électronique faisant l'objet de la notification préalable en vue de sa présentation au groupe de coopération par l'État membre ayant procédé à la notification préalable.

2. Le président du groupe de coopération veille à ce que la réunion programmée visée au paragraphe 1 ait lieu au plus tard deux mois après que le groupe de coopération a été informé du déclenchement de l'examen par les pairs.

3. La date de la présentation est considérée comme la date officielle de début de l'examen par les pairs.

4. Après que l'État membre ayant procédé à la notification préalable a effectué la présentation visée au paragraphe 3, les autres États membres peuvent désigner des représentants chargés de participer à l'examen par les pairs en leur nom. Dans ce cas, ils fournissent les noms et coordonnées de leurs représentants. Ces représentants désignés forment le groupe d'examen par les pairs.

Les membres du groupe d'examen par les pairs s'accordent sur l'attribution des rôles suivants:

a) un coordinateur chargé d'organiser l'examen par les pairs et de gérer la communication avec les États membres, le groupe de coopération et la Commission;

b) jusqu'à trois rapporteurs en fonction de l'étendue de l'examen par les pairs, dont chacun dirige un groupe de travail visé à l'article 4, paragraphe 2;

c) au moins un membre actif par groupe de travail, qui aide à générer des questions et à fournir un retour d'information aux rapporteurs et contribue à l'élaboration du rapport final d'examen par les pairs.

5. Le coordinateur visé au paragraphe 4, point a), supervise la bonne exécution de l'examen par les pairs et contrôle le respect des exigences procédurales énoncées dans le présent règlement. À cette fin, le coordinateur s'acquitte en temps utile des tâches suivantes:

a) organisation des questions et réponses;

b) finalisation du rapport d'examen par les pairs;

c) élaboration de l'avis sur le schéma d'identification électronique faisant l'objet de l'évaluation par les pairs.

6. Les rapporteurs visés au paragraphe 4, point b), établissent les questions destinées à l'État membre ayant procédé à la notification préalable et rédigent les éléments du rapport d'examen par les pairs qui se rapportent au domaine de compétence de leur groupe de travail respectif.

7. Compte tenu des orientations fournies par le groupe de coopération, l'État membre ayant procédé à la notification préalable et les États membres participant à l'examen par les pairs conviennent de toute modalité organisationnelle relative à l'examen par les pairs qui n'est pas expressément prévue par le présent règlement, comprenant les règles et les lignes directrices relatives à la confidentialité et aux conflits d'intérêts.

8. La durée de l'examen par les pairs ne dépasse pas trois mois à compter de la date officielle de début de l'examen par les pairs visée au paragraphe 3 et peut être prolongée de deux mois au maximum si tous les États membres participant à l'examen par les pairs s'accordent sur ce point.

Article 4

Organisation de l'examen par les pairs

1. Le groupe d'examen par les pairs procède à l'examen par les pairs à partir des informations fournies en application de l'article 2, paragraphe 1, par l'État membre ayant effectué la notification préalable.

2. L'examen par les pairs est organisé en trois groupes de travail ou selon tout autre mode opératoire déterminé au sein du groupe de coopération conformément à son règlement intérieur. S'il est fait appel à des groupes de travail, chacun d'eux est composé d'un rapporteur et d'au moins un membre actif.

3. Les groupes de travail visés au paragraphe 2 sont les suivants:

a) un groupe de travail sur l'inscription, qui procède à l'examen par les pairs de la concordance entre le schéma d'identification électronique ayant fait l'objet de la notification préalable et les exigences relatives à l'inscription énoncées au point 2.1 de l'annexe du règlement d'exécution (UE) 2015/1502;

b) un groupe de travail sur la gestion des moyens d'identification électronique et l'authentification, qui procède à l'examen par les pairs de la concordance entre le schéma d'identification électronique faisant l'objet de la notification préalable et les exigences relatives à la gestion des moyens d'identification électronique et à l'authentification énoncées aux points 2.2 et 2.3 de l'annexe du règlement d'exécution (UE) 1502/2015;

c) un groupe de travail sur la gestion et l'organisation, qui procède à l'examen par les pairs de la concordance entre le schéma d'identification électronique faisant l'objet de la notification préalable et les exigences relatives à la gestion et à l'organisation énoncées au point 2.4 du règlement d'exécution (UE) 2015/1502.

4. L'examen par les pairs comprend, sans s'y limiter, une ou plusieurs des activités suivantes:

a) l'évaluation des documents utiles fournis par l'État membre ayant procédé à la notification préalable;

b) l'examen des processus décrits dans le cadre de ces documents;

c) des séminaires techniques;

d) la prise en compte des évaluations réalisées par des tiers indépendants, s'il existe des évaluations utiles de ce type;

e) la rédaction du rapport d'examen par les pairs qui résume les conclusions et les résultats de l'examen par les pairs.

5. Les groupes de travail peuvent adresser des demandes dûment justifiées d'informations supplémentaires, étayées par des documents supplémentaires, à l'État membre ayant procédé à la notification préalable lorsque les informations fournies conformément à l'article 2, paragraphe 1, ne sont pas suffisantes pour clore l'examen par les pairs.

6. L'État membre ayant procédé à la notification préalable satisfait à ces demandes, sauf si l'une des situations suivantes se présente:

a) les informations ou documents ne sont pas en sa possession et se les procurer créerait une charge administrative excessive;

b) les informations ou documents demandés ont trait à des questions de sécurité publique ou nationale;

c) les informations se rapportent à des affaires commerciales ou ont trait au secret professionnel ou industriel;

d) le caractère sensible des informations rend impossible la mise en place d'un canal sécurisé permettant de communiquer les informations aux membres du groupe d'évaluation par les pairs.

7. En pareil cas, l'État membre ayant procédé à la notification préalable informe le coordinateur des raisons pour lesquelles il refuse de fournir les informations ou les documents demandés et soumet une synthèse générale des informations ou une version expurgée des documents.

Article 5

Résultat de l'examen par les pairs

1. Sans préjudice de l'article 3, paragraphe 9, le groupe d'examen par les pairs:

a) fournit un projet de rapport d'examen par les pairs à l'État membre ayant procédé à la notification préalable au plus tard trois mois après la date de début de l'examen par les pairs visée à l'article 3, paragraphe 3, sauf si l'examen par les pairs fait l'objet d'une prolongation conformément à l'article 3, paragraphe 8, auquel cas la date de communication du rapport est fonction de la prolongation convenue;

b) fournit le projet de rapport final d'examen par les pairs à la Commission et au groupe de coopération, après avoir pris en considération les observations éventuelles de l'État membre ayant procédé à la notification préalable sur le contenu du projet de rapport d'examen par les pairs, au plus tard trois mois et deux semaines après la date officielle de début de l'examen par les pairs prévue à l'article 3, paragraphe 3, sauf si l'examen par les pairs fait l'objet d'une prolongation conformément à l'article 3, paragraphe 8, auquel cas la date de communication du rapport est fonction de la prolongation convenue;

c) fournit à l'État membre ayant procédé à la notification préalable un projet d'avis sur le schéma d'identification électronique faisant l'objet de la notification préalable au plus tard trois mois et deux semaines après la date officielle de début de l'examen par les pairs visée à l'article 3, paragraphe 3, sauf si l'examen par les pairs fait l'objet d'une prolongation conformément à l'article 3, paragraphe 8, auquel cas la date de communication de l'avis est fonction de la prolongation convenue, et élabore le projet d'avis en utilisant le modèle figurant à l'annexe IV;

d) fournit à la Commission et au groupe de coopération un projet d'avis final sur le schéma d'identification électronique faisant l'objet de la notification préalable au plus tard trois mois et trois semaines après la date de début de l'examen par les pairs visée à l'article 3, paragraphe 3, sauf si l'examen par les pairs fait l'objet d'une prolongation conformément à l'article 3, paragraphe 8, auquel cas la date de communication de l'avis est fonction de la prolongation convenue.

2. Avant d'adopter et de publier, sur un site web dédié de la Commission, son avis final sur la conclusion de l'examen par les pairs conformément au paragraphe 9, le groupe de coopération peut demander des informations ou des éclaircissements supplémentaires à l'État membre ayant procédé à la notification préalable ou au groupe d'examen par les pairs.

3. L'État membre ayant procédé à la notification préalable fournit les informations supplémentaires demandées en application du paragraphe 2, sauf si l'une des situations suivantes se présente:

a) les informations ne sont pas en sa possession et se les procurer créerait une charge administrative excessive;

b) les informations ont trait à des questions de sécurité publique ou nationale;

c) les informations ont trait au secret commercial, professionnel ou industriel.

d) le caractère sensible des informations rend impossible la mise en place d'un canal sécurisé permettant de les communiquer au groupe de coopération.

4. Le rapport final d'examen par les pairs fournit la liste des informations qui ont été demandées par le groupe d'examen par les pairs ou par le groupe de coopération mais qui n'ont pas pu être fournies pour un ou plusieurs des motifs énoncés au paragraphe 3, sans préciser les raisons avancées par l'État membre ayant procédé à la notification préalable. L'incidence de toute indisponibilité d'informations peut être examinée par le groupe d'examen par les pairs dans le rapport final d'examen par les pairs.

5. Le groupe d'examen par les pairs présente le rapport final d'examen par les pairs et son projet d'avis final au groupe de coopération au plus tard quatre mois ou, en cas de prolongation conformément à l'article 3, paragraphe 8, au plus tard six mois après la date officielle de début de l'examen par les pairs visée à l'article 3, paragraphe 3.

6. L'avis final du groupe d'examen par les pairs sur le schéma d'identification électronique de l'État membre ayant procédé à la notification préalable comprend la liste des engagements éventuels pris par cet État membre.

7. Après la présentation du rapport final d'examen par les pairs et de l'avis final du groupe d'examen par les pairs, le groupe de coopération adopte et publie son propre avis sur la conclusion de l'examen par les pairs, en indiquant si et comment le schéma d'identification électronique ayant fait l'objet de l'évaluation par les pairs satisfait aux exigences énoncées dans le règlement d'exécution (UE) 2015/1502 qui s'appliquent aux niveaux de garantie indiqués par l'État membre ayant procédé à la notification préalable, conformément à l'annexe I du présent règlement. Le processus d'adoption respecte le règlement intérieur du groupe de coopération.

8. L'avis du groupe de coopération identifie l'État membre ayant procédé à la notification préalable ainsi que le schéma d'identification électronique ainsi notifié et son niveau de garantie. L'avis indique également si l'examen par les pairs a été accompli avec succès.

9. Les informations fournies en application de l'article 2, paragraphe 1, sont publiées par le groupe de coopération, sauf si l'État membre qui les a fournies a indiqué par écrit que ces informations ne devaient pas être rendues publiques.

Article 6

Modifications importantes des schémas d'identification électronique ayant fait l'objet d'une évaluation par les pairs

1. Lorsqu'un schéma d'identification électronique notifié est modifié d'une manière susceptible d'avoir une incidence sur son interopérabilité, sa sécurité ou sa fiabilité, l'État membre qui a procédé à la notification communique sans retard injustifié ces modifications au groupe de coopération et met à jour les informations fournies précédemment.

2. Après réception d'une notification visée au paragraphe 1, et dans la mesure où le schéma d'identification électronique notifié a fait l'objet d'un examen par les pairs, tout État membre du groupe de coopération peut demander une mise à jour de l'examen par les pairs.

3. En cas de demande de mise à jour, les procédures prévues aux articles 3 à 5 s'appliquent en conséquence et le groupe d'examen par les pairs limite l'examen par les pairs aux éléments qui ont été modifiés au regard de la notification initiale et des incidences de ces modifications.

Article 7

Abrogation

La décision d'exécution (UE) 2015/296 est abrogée.

Article 8

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 juillet 2025.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE I

Liste des informations minimales à fournir dans la table de correspondance des niveaux de garantie pour l'examen par les pairs visée à l'article 2, paragraphe 1, point a)

La table de correspondance des niveaux de garantie pour l'examen par les pairs visée à l'article 2, paragraphe 1, point a), comprend au moins les informations suivantes:

1) des informations générales, y compris:

   a) le nom de l'État membre auteur de la notification;

   b) l'intitulé du schéma d'identification électronique (le cas échéant);

   c) le ou les niveaux de garantie du schéma d'identification électronique, accompagnés de la mention «faible», «substantiel» ou «élevé»;

2) l'autorité ou les autorités responsables du schéma d'identification électronique, y compris:

   a) le ou les noms de l'autorité ou des autorités responsables du schéma d'identification électronique;

   b) l'adresse électronique de l'autorité ou des autorités responsables du schéma d'identification électronique;

3) des informations sur les parties, entités et organismes concernés associés au schéma d'identification électronique, y compris:

   a) le nom de l'entité ou des entités qui gèrent le processus d'enregistrement des données d'identification personnelle uniques;

   b) le nom de la partie ou des parties délivrant le moyen d'identification électronique et, le cas échéant, une mention indiquant si la ou les parties sont visées à l'article 7, point a), i), ii) ou iii), du règlement (UE) nº 910/2014;

   c) le nom de la partie ou des parties qui gèrent la procédure d'authentification (le «nœud eIDAS»);

   d) le ou les noms de l'organisme ou des organismes de gouvernance participant au régime de contrôle lié au schéma d'identification électronique;

4) une description du schéma d'identification électronique, y compris:

   a) le cas échéant, le ou les documents à joindre pour chacun des points suivants:

      — une brève description du schéma d'identification électronique, y compris le contexte dans lequel il fonctionne, son champ d'application et sa disponibilité pour les parties utilisatrices privées,

      — une liste des attributs supplémentaires qui peuvent être prévus pour les personnes physiques au titre du schéma d'identification électronique si une partie utilisatrice le demande,

      — une liste des attributs supplémentaires qui peuvent être prévus pour les personnes morales au titre du schéma d'identification électronique si une partie utilisatrice le demande;

   b) le régime applicable en matière de contrôle, de responsabilité et de gestion, y compris:

      — une description du régime de contrôle du schéma d'identification électronique, y compris le processus d'évaluation en ce qui concerne:

         — le régime de contrôle applicable à la partie ou aux parties délivrant le moyen d'identification électronique,

         — le régime de contrôle applicable à la partie ou aux parties gérant le nœud eIDAS.

Le cas échéant, ces descriptions font ressortir les rôles, les responsabilités et les pouvoirs des organismes de gouvernance qui participent au régime de contrôle visés au point 3), d), ainsi que de l'entité à laquelle ils rendent compte. Si les organismes ne rendent pas compte à l'autorité responsable du schéma, les coordonnées complètes de l'entité à laquelle ils rendent compte doivent également être fournies;

— une description du régime national de responsabilité applicable, y compris:

  — une description de la responsabilité de l'État membre en vertu de l'article 11, paragraphe 1, du règlement (UE) nº 910/2014,

  — une description de la responsabilité de la ou des parties délivrant les moyens d'identification électronique en vertu de l'article 11, paragraphe 2, du règlement (UE) nº 910/2014,

  — une description de la responsabilité de la ou des parties gérant le nœud eIDAS en vertu de l'article 11, paragraphe 3, du règlement (UE) nº 910/2014,

— les modalités de gestion, de suspension ou de révocation soit de l'ensemble du schéma d'identification, soit de moyens d'identification électronique spécifiques, soit du nœud eIDAS, ou de leurs éléments altérés;

c) une description des composants du schéma d'identification électronique, y compris:

— une description de la manière dont sont remplies les exigences concernant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique, énoncées dans le règlement d'exécution (UE) 2015/1502, afin de justifier le niveau de garantie indiqué pour l'inscription,

— une description de la manière dont les processus suivants sont pris en charge dans le cadre du schéma d'identification électronique, y compris la documentation relative à la combinaison des options choisies par l'État membre, en matière de:

  — demande et enregistrement,

  — preuve et vérification d'identité d'une personne physique,

  — preuve et vérification d'identité d'une personne morale,

  — lien établi entre les moyens d'identification électronique de personnes physiques et morales,

— en ce qui concerne la gestion des moyens d'identification électronique, une description de la manière dont les processus suivants sont pris en charge dans le cadre des moyens d'identification électronique:

  — les caractéristiques et la conception des moyens d'identification électronique, y compris, le cas échéant, les informations relatives à la certification de sécurité,

  — la délivrance, la mise à disposition et l'activation,

  — la suspension, la révocation et la réactivation,

  — le renouvellement et le remplacement,

— en ce qui concerne l'authentification, une description du mécanisme d'authentification, y compris les conditions d'accès à l'authentification par les parties utilisatrices autres que les organismes du secteur public,

— en ce qui concerne la gestion et l'organisation, une description de la gestion et de l'organisation des aspects suivants:

  — dispositions générales concernant la gestion et l'organisation,

  — avis publiés et information des utilisateurs,

  — gestion de la sécurité de l'information,

  — conservation d'informations,

— installations et personnel,

— contrôles techniques,

— conformité et audit;

d) une description de la manière dont sont remplies les exigences d'interopérabilité et les exigences minimales de sécurité technique et opérationnelle;

e) une liste de toutes les pièces justificatives présentées et une déclaration précisant auxquels des éléments ci-dessus elles se rapportent, y compris les références à toute législation nationale qui porte sur la disposition en matière d'identification électronique qui est en rapport avec la notification ainsi que les rapports d'audit, les énoncés des pratiques de certification et les rapports d'essai pertinents;

f) les documents et informations pertinents concernant la certification du schéma d'identification électronique conformément à l'article 12 *bis*, paragraphe 1, et, le cas échéant, à l'article 12 *bis*, paragraphe 5, du règlement (UE) nº 910/2014.

ANNEXE II

Liste des informations minimales à fournir dans le livre blanc visé à l'article 2, paragraphe 1, point b)

1. Le livre blanc décrit l'écosystème global du schéma d'identification électronique faisant l'objet d'une notification préalable, ainsi que l'historique du schéma d'identification électronique et de l'identification électronique dans l'État membre.

2. Le livre blanc fournit également une description du schéma d'identification électronique et des moyens d'identification électronique fournis dans le cadre de ce schéma, comprenant une brève description des éléments qui sont également couverts par la table de correspondance des niveaux de garantie visée à l'article 2, paragraphe 1, point a), du présent règlement, la table de correspondance du cadre d'interopérabilité visé à l'article 2, paragraphe 1, point c), du présent règlement, ainsi que d'autres documents.

3. Le livre blanc décrit également le rôle du schéma d'identification électronique dans l'écosystème global et son rapport avec les parties utilisatrices et les autres services fournis au sein de l'écosystème.

ANNEXE III

Modèle de table de correspondance du cadre d'interopérabilité

Exigences d'interopérabilité

Article du règlement d'exécution (UE) 2015/1501	Exigence	Description
4	**Table de correspondance des niveaux de garantie nationaux** L'établissement de la table de correspondance des niveaux de garantie nationaux des schémas d'identification électronique notifiés respecte les exigences du règlement d'exécution (UE) 2015/1502. Les résultats sont notifiés à la Commission au moyen du modèle de notification établi dans la décision d'exécution (UE) 2015/1984.	<À remplir par l'État membre>
5	**Nœuds** 1. Un nœud situé dans un État membre doit être en mesure de communiquer avec les nœuds d'autres États membres. 2. Les nœuds doivent être en mesure de faire la distinction entre les organismes du secteur public et les autres parties utilisatrices par le biais de moyens techniques. 3. La mise en œuvre par un État membre des exigences techniques énoncées dans le présent règlement ne doit pas avoir pour effet d'imposer aux autres États membres qui souhaitent interopérer avec cette mise en œuvre des exigences techniques et des coûts disproportionnés.	<À remplir par l'État membre>
6	**Respect de la vie privée et confidentialité des données** 1. Le respect de la vie privée, la confidentialité des données échangées et le maintien de l'intégrité des données entre les nœuds sont assurés au moyen des meilleures solutions techniques et pratiques de protection disponibles. 2. Les nœuds ne peuvent stocker aucune donnée personnelle, excepté aux fins de l'article 9, paragraphe 3, du règlement d'exécution (UE) 2015/1501.	<À remplir par l'État membre>
7	**Intégrité et authenticité des données dans le cadre de la communication** La communication entre les nœuds assure l'intégrité et l'authenticité des données de manière à garantir que toutes les demandes et réponses sont authentiques et n'ont pas fait l'objet de manipulations non autorisées. À cette fin, les nœuds ont recours à des solutions qui ont été utilisées avec succès dans le cadre d'une utilisation opérationnelle transfrontalière.	<À remplir par l'État membre>

Article du règlement d'exécution (UE) 2015/1501	Exigence	Description
8	**Format des messages dans le cadre de la communication** La syntaxe utilisée par les nœuds est celle de formats de message communs fondés sur des normes dont on recense plusieurs exemples de déploiement entre les États membres et dont la capacité de fonctionnement dans un environnement opérationnel est prouvée. La syntaxe permet: a) de traiter convenablement l'ensemble minimal de données d'identification personnelle représentant de façon univoque une personne physique ou morale; b) de traiter convenablement le niveau de garantie du moyen d'identification électronique; c) d'établir la distinction entre les organismes du secteur public et les autres parties utilisatrices; d) de disposer de la flexibilité nécessaire pour répondre aux besoins d'attributs supplémentaires relatifs à l'identification.	<À remplir par l'État membre>
9	**Gestion des informations de sécurité et des métadonnées** 1. L'opérateur de nœud communique les métadonnées relatives à la gestion de nœud sous un format normalisé traitable par machine et d'une façon sûre et digne de confiance. 2. Les paramètres relatifs à la sécurité, au moins, doivent pouvoir être récupérés automatiquement. 3. L'opérateur de nœud stocke des données qui, en cas d'incident, permettent de reconstruire la séquence de l'échange de messages pour déterminer le lieu et la nature de l'incident. Les données sont stockées pendant une durée conforme aux exigences nationales et comportent, au minimum, les éléments suivants: a) identification du nœud; b) identification du message; c) date et heure du message.	<À remplir par l'État membre>
10	**Normes d'assurance et de sécurité de l'information** 1. Les opérateurs de nœuds assurant une authentification apportent la preuve que, eu égard aux nœuds participant au cadre d'interopérabilité, le nœud respecte les exigences de la norme ISO/CEI 27001 par certification, par des méthodes d'évaluation équivalentes ou par conformité à la législation nationale. 2. Les opérateurs de nœuds déploient les mises à jour de sécurité critiques sans retard injustifié.	<À remplir par l'État membre>

Article du règlement d'exécution (UE) 2015/1501	Exigence	Description
11	**Données d'identification personnelle** 1. Lorsqu'un ensemble minimal de données d'identification personnelle représentant de façon univoque une personne physique ou morale est utilisé dans un contexte transfrontalier, il respecte les exigences visées à l'annexe du règlement d'exécution (UE) 2015/1501. 2. Lorsqu'un ensemble minimal de données pour une personne physique représentant une personne morale est utilisé dans un contexte transfrontalier, il contient la combinaison des attributs énumérés à l'annexe du règlement d'exécution (UE) 2015/1501 pour les personnes physiques et les personnes morales. 3. Les données sont transmises sur la base des caractères d'origine et, le cas échéant, également transcrites en caractères latins.	<À remplir par l'État membre>

ANNEXE IV

Modèle d'avis sur le schéma d'identification électronique d'un État membre

Avis n° XX/202X du groupe de coopération sur le schéma d'identification électronique <insérer le nom du schéma> de <insérer le nom de l'État membre>

Vu l'article 12, paragraphe 5, du règlement (UE) n° 910/2014 (ci-après le «règlement concernant un cadre européen relatif à une identité numérique»),

vu le règlement d'exécution (UE) 2025/1568,

vu le règlement intérieur du groupe de coopération,

considérant ce qui suit:

L'article 12, paragraphe 5, du règlement concernant un cadre européen relatif à une identité numérique oblige les États membres à procéder à des examens par les pairs des schémas d'identification électronique qui doivent être notifiés en vertu de son article 9, paragraphe 1, point a).

L'article 5, paragraphe 10, du règlement d'exécution (UE) 2025/1568 relatif à la coopération charge le groupe de coopération d'adopter des avis sur la façon dont un schéma d'identification électronique qui doit être notifié satisfait aux exigences du règlement concernant un cadre européen relatif à une identité numérique.

<Insérer le nom de l'État membre>, en vue de notifier son schéma d'identification électronique <insérer le nom du schéma> conformément à l'article 9, paragraphe 1, du règlement concernant un cadre européen relatif à une identité numérique, a fourni le <insérer la date> aux États membres les informations suivantes (ci-après: «notification préalable») en application de l'article 7, point g), du règlement concernant un cadre européen relatif à une identité numérique:

— *formulaire de notification,*

— *pièces justificatives.*

Le <insérer la date de la réunion du GC>, le groupe de coopération:

— *a décidé d'organiser l'examen par les pairs du schéma d'identification électronique <insérer le nom du schéma> de <insérer le nom de l'État membre> conformément à l'article 46 sexies, paragraphe 5, point d), du règlement concernant un cadre européen relatif à une identité numérique et au règlement d'exécution (UE) 2025/1568,*

— *a formé un «groupe d'examen par les pairs», et*

— *a arrêté les points couverts par le processus d'examen par les pairs et la manière dont il serait organisé conformément aux dispositions du règlement d'exécution (UE) 2025/1568.*

Le <insérer la date>, le groupe d'évaluation par les pairs a soumis son rapport au groupe de coopération conformément à l'article 5 du règlement d'exécution (UE) 2025/1568. Le groupe de coopération a examiné et discuté le rapport d'évaluation par les pairs.

Compte tenu des résultats de l'examen par les pairs, du rapport d'examen par les pairs et des informations supplémentaires fournies par <insérer le nom de l'État membre> en ce qui concerne:

—

et du fait que <insérer le nom de l'État membre> s'engage à:

—

le groupe de coopération adopte l'avis suivant:

Avis

Sur la base de l'examen des documents de notification préalable fournis par <insérer le nom de l'État membre> et des conclusions du rapport d'examen par les pairs, le groupe de coopération est d'avis que les documents de notification préalable et les informations supplémentaires fournies par <insérer le nom de l'État membre> démontrent à suffisance la façon dont le schéma d'identification électronique <insérer le nom du schéma> de <insérer le nom de l'État membre> qui doit être notifié satisfait aux exigences.

— *pour le niveau de garantie «élevé»,*

— *pour le niveau de garantie «substantiel»,*

— *pour le niveau de garantie «faible»,*

conformément aux exigences de l'article 7, de l'article 8, paragraphes 1 et 2, de l'article 12, paragraphe 1, et de l'article 12 bis*, paragraphes 1 et 5, du règlement concernant un cadre européen relatif à une identité numérique et aux exigences du règlement d'exécution (UE) 2015/1502.*

Conformément à l'article <insérer le numéro> du règlement intérieur, le groupe de coopération convient de publier le présent avis.

<insérer le nom de l'État membre>, <insérer la date>

Journal officiel
de l'Union européenne

FR
Série L

2025/1569

30.7.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/1569 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 attestations électroniques d'attributs qualifiées et les attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte

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 *quinquies*, paragraphe 5, son article 45 *sexies*, paragraphe 2, et son article 45 *septies*, paragraphes 6 et 7,

considérant ce qui suit:

(1) Le règlement (UE) nº 910/2014 a créé un cadre juridique pour la délivrance et la validation des attestations électroniques d'attributs, imposant notamment aux fournisseurs d'attestations électroniques d'attributs d'offrir aux utilisateurs de portefeuilles européens d'identité numérique (ci-après les «portefeuilles») la possibilité de demander, d'obtenir, de stocker et de gérer les attestations électroniques d'attributs, indépendamment de l'État membre dans lequel les portefeuilles sont fournis. Les attestations électroniques d'attributs sont des éléments essentiels pour la mise en place d'un écosystème des portefeuilles européens d'identité numérique (ci-après l'«écosystème des portefeuilles») sécurisé et interopérable. Elles permettent aux utilisateurs de partager des informations avec les parties utilisatrices de manière fiable dans divers cas d'utilisation.

(2) Les interfaces avec les portefeuilles européens d'identité numérique que doivent fournir les fournisseurs d'attestations électroniques d'attributs qualifiées conformément à l'article 45 *octies* du règlement (UE) nº 910/2014 mettent en évidence l'importance que revêtent les attestations électroniques d'attributs pour l'écosystème des portefeuilles et facilitent leur adoption rapide.

(3) La Commission évalue régulièrement les nouvelles technologies, pratiques, normes et spécifications techniques. Afin d'atteindre le niveau d'harmonisation le plus élevé possible entre les États membres en ce qui concerne le développement et la certification des portefeuilles, les spécifications techniques énoncées dans le présent règlement s'appuient sur les travaux menés au titre de la recommandation (UE) 2021/946 de la Commission du 3 juin 2021 concernant une boîte à outils commune de l'Union pour une approche coordonnée en vue d'un cadre européen relatif à une identité numérique ([2]), et en particulier sur l'architecture et le cadre de référence qui sont une composante de cette boîte à outils. Conformément au considérant 75 du règlement (UE) 2024/1183 du Parlement européen et du Conseil ([3]), la Commission devrait réexaminer et, si besoin est, mettre à jour le présent règlement, afin de le maintenir en adéquation avec les évolutions générales, l'architecture et le cadre de référence et de suivre les meilleures pratiques sur le marché intérieur, notamment en ce qui concerne la délivrance d'attestations électroniques d'attributs et la vérification des attributs par rapport aux sources authentiques ou via des intermédiaires désignés.

(4) Lorsque les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte délivrent des attestations censées être conformes aux exigences des programmes d'attestation d'attributs enregistrés dans le catalogue, les règles et procédures visant à garantir le respect des exigences de ces programmes devraient faire partie de l'évaluation de la conformité prévue par le règlement (UE) nº 910/2014.

([1]) JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) JO L 210 du 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.
([3]) 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).

(5) La protection contre les informations peu fiables revêt une grande importance pour la dématérialisation des attestations. Par conséquent, les attestations électroniques d'attributs qualifiées et les attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte devraient pouvoir être révoquées, ou d'autres mesures devraient être mises en œuvre pour compenser les risques liés à l'impossibilité de les révoquer. Certaines circonstances devraient entraîner la révocation d'une attestation électronique d'attributs par le fournisseur, par exemple lorsque la personne à qui l'attestation électronique d'attributs a été délivrée en fait la demande explicite, lorsque le fournisseur sait que la sécurité ou la fiabilité des attestations électroniques d'attributs qualifiées a été compromise, ou lorsque le droit de l'Union ou le droit national l'exige. Afin de protéger les droits fondamentaux de l'utilisateur au respect de la vie privée et à la protection des données, notamment en réduisant de manière appropriée les risques liés à l'associabilité et à la traçabilité, les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte devraient mettre en place des règles de gestion des révocations respectueuses de la vie privée.

(6) Pour faciliter la coopération entre les États membres et la création d'un écosystème d'identité numérique sécurisé et interopérable, y compris la reconnaissance transfrontière et l'interopérabilité des attestations électroniques d'attributs qualifiées et des attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte, il est nécessaire de mettre en place des procédures de communication administrative simplifiées entre les parties prenantes concernées comprenant notamment la publication d'informations permettant d'identifier rapidement les organismes du secteur public pertinents. Les États membres devraient notifier les attributs concernés à la Commission. Pour que la vérification de ces attributs puisse se faire sans délai, de manière efficace et interopérable, les notifications pertinentes adressées à la Commission devraient être au moins en anglais, car cela les rend plus accessibles et plus faciles à évaluer et à comprendre, tout en renforçant la coopération entre les parties prenantes concernées. Il convient toutefois que la traduction des documents préexistants n'entraîne pas de charges administratives ou financières déraisonnables.

(7) Pour permettre aux utilisateurs et aux prestataires de services de vérifier que les attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte ont bien été délivrées par l'organisme du secteur public en question ou pour son compte, les États membres devraient notifier à la Commission la liste de ces organismes du secteur public. Lorsqu'ils notifient la liste des organismes du secteur public qui délivrent des attestations électroniques d'attributs conformément à l'article 45 *septies* et à l'annexe VII du règlement (UE) nº 910/2014, les États membres doivent fournir un rapport d'évaluation de la conformité confirmant que ces organismes présentent un niveau de fiabilité équivalent à celui des prestataires de services de confiance qualifiés. Toutefois, dans le cas des organismes du secteur public, contrairement aux prestataires de services de confiance qualifiés délivrant des attestations électroniques d'attributs qualifiées, ce sont les États membres qui décident comment ils garantissent que les prestataires satisfont aux exigences au fil du temps. Pour que la confiance dans les attestations délivrées par des organismes du secteur public se maintienne à un niveau élevé dans l'ensemble de l'Union, les États membres sont encouragés à partager leurs bonnes pratiques en matière de garantie permanente de la fiabilité par l'intermédiaire du groupe de coopération européen en matière d'identité numérique (ci-après le «groupe de coopération») établi en vertu de l'article 46 *sexies*, paragraphe 1, du règlement (UE) nº 910/2014. La Commission devrait établir, tenir à jour et publier une liste des prestataires et faire en sorte que cette liste soit facilement accessible au public.

(8) La Commission, avec l'aide du groupe de coopération, devrait établir un catalogue d'attributs afin de faciliter la vérification des attributs par rapport aux sources authentiques par les prestataires de services de confiance qualifiés délivrant des attestations électroniques d'attributs qualifiées. L'enregistrement des attributs énumérés à l'annexe VI du règlement (UE) nº 910/2014 dans le catalogue d'attributs devrait être obligatoire. Pour les autres attributs, l'enregistrement serait facultatif.

(9) La Commission, avec l'aide du groupe de coopération, devrait établir un catalogue de programmes d'attestation d'attributs afin de faciliter la délivrance des attestations par les prestataires de services de confiance qualifiés délivrant des attestations électroniques d'attributs qualifiées et par les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte, ainsi que pour contribuer à l'harmonisation et à l'interopérabilité transfrontière de ces attestations. L'enregistrement des programmes dans le catalogue de programmes devrait être facultatif. Les demandes d'enregistrement ou de modification d'attributs dans le catalogue devraient être introduites par le propriétaire du programme d'attestation d'attributs et peuvent inclure des attributs qui ne figurent pas dans le catalogue d'attributs. La Commission devrait évaluer ces demandes en tenant compte des besoins en matière d'interopérabilité et d'harmonisation.

(10) Afin de faire en sorte que le catalogue d'attributs contienne des informations utiles et atteigne un niveau élevé d'interopérabilité au sein de l'écosystème des attestations électroniques d'attributs, il devrait fournir un ensemble minimal d'informations, telles qu'une description sémantique de l'attribut, l'espace de nom auquel appartient son identifiant et le type de données de l'attribut. À cette même fin, le catalogue de programmes d'attestation d'attributs devrait contenir des descriptions des types fréquents d'attestations électroniques d'attributs ainsi qu'une description du modèle de confiance et des mécanismes de gouvernance appliqués dans le cadre du programme d'attestation. Les informations figurant dans les catalogues devraient comprendre la version des attributs et des programmes afin que les attestations délivrées pour des versions précises ne soient pas affectées par des modifications apportées à ces attributs et programmes.

(11) Pour garantir l'efficacité de la vérification des attributs par rapport aux sources authentiques par les prestataires de services de confiance qualifiés délivrant des attestations électroniques d'attributs qualifiées, y compris via des intermédiaires désignés qui fournissent des mécanismes de vérification indirecte aux prestataires de services, les États membres devraient mettre en place, dans le délai fixé à l'article 45 *sexies*, paragraphe 1, du règlement (UE) nº 910/2014, des mécanismes permettant aux prestataires de services de confiance qualifiés délivrant des attestations électroniques d'attributs qualifiées de demander la vérification des attributs. Ces mécanismes devraient permettre aux prestataires de services de confiance qualifiés délivrant des attestations électroniques d'attributs qualifiées de déterminer quels attributs peuvent être vérifiés et de quelle manière il convient de le faire. Ces mécanismes devraient inclure des précisions sur les points d'accès et les protocoles de service permettant de vérifier la validité et l'exactitude des attributs. Il convient également d'envisager la possibilité de proposer un point de vérification unique au niveau national.

(12) Plus précisément, les États membres devraient mettre à la disposition des prestataires de services de confiance qualifiés délivrant des attestations électroniques d'attributs qualifiées les mécanismes permettant d'accéder aux points de vérification au niveau national pour chacun des attributs énumérés à l'annexe VI du règlement (UE) nº 910/2014 et de les utiliser. Ces mécanismes devraient permettre aux prestataires de services de confiance qualifiés délivrant des attestations électroniques d'attributs qualifiées de présenter, à la demande de l'utilisateur, des attributs spécifiques à un point de vérification en vue de la délivrance de l'attestation et pendant la durée de vie de celle-ci. Les mécanismes de vérification devraient faire appel à des moyens électroniques adaptés au traitement automatique et permettant d'obtenir une réponse du point de vérification le plus rapidement possible. Cette réponse devrait permettre de confirmer si les attributs présentés par les prestataires de services de confiance qualifiés délivrant des attestations électroniques d'attributs qualifiées correspondent aux attributs stockés dans la source authentique concernée pour cet utilisateur et indiquer la source authentique utilisée pour la vérification. Pour éviter les abus, tels que les demandes de vérification illicites ou manifestement excessives, les États membres peuvent, lorsqu'ils le jugent approprié, imposer des mécanismes de contrôle de l'utilisation des points de vérification, en tenant compte de facteurs pertinents, par exemple du fait que les sources authentiques contiennent des informations qui devraient être considérées comme des données à caractère personnel ou qui sont de nature confidentielle ou sensible en vertu du droit de l'Union ou du droit national.

(13) Conformément aux principes énoncés par le règlement pour une Europe interopérable ([4]), afin de faciliter l'établissement du catalogue d'attributs et du catalogue de programmes d'attestation d'attributs ainsi que la réutilisation, dans la mesure du possible, des informations, catalogues et programmes existants, la Commission devrait, lorsqu'il y a lieu, exploiter les synergies avec les services communs du système technique institué par le règlement (UE) 2018/1724 du Parlement européen et du Conseil établissant un portail numérique unique et modifiant le règlement (UE) nº 1024/2012 ([5]).

(14) Afin d'améliorer l'interopérabilité des attestations électroniques d'attributs délivrées par des prestataires de services de confiance non qualifiés, les entités délivrant les attestations peuvent suivre les principes et exigences applicables aux attestations électroniques d'attributs non qualifiées définis dans le présent règlement.

([4]) Règlement (UE) 2024/903 du Parlement européen et du Conseil du 13 mars 2024 établissant des mesures destinées à assurer un niveau élevé d'interopérabilité du secteur public dans l'ensemble de l'Union (règlement pour une Europe interopérable) (JO L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

([5]) Règlement (UE) 2018/1724 du Parlement européen et du Conseil du 2 octobre 2018 établissant un portail numérique unique pour donner accès à des informations, à des procédures et à des services d'assistance et de résolution de problèmes, et modifiant le règlement (UE) nº 1024/2012 (JO L 295 du 21.11.2018, p. 1, ELI: http://data.europa.eu/eli/reg/2018/1724/oj).

(15) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([6]) et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([7]) s'appliquent aux activités de traitement de données à caractère personnel au titre du présent règlement.

(16) Afin d'accorder à la Commission et aux États membres suffisamment de temps pour dresser la liste des fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte, les exigences du présent règlement concernant le catalogue d'attributs, le catalogue de programmes d'attestation d'attributs et les points de vérification des attributs devraient devenir applicables 12 mois après la date d'entrée en vigueur du présent règlement.

(17) 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 ([8]) et a rendu son avis le 31 janvier 2025.

(18) Les mesures prévues par le présent règlement sont conformes à l'avis du comité institué par l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Objet et champ d'application

Le présent règlement établit les normes de référence, spécifications et procédures qui s'appliquent aux éléments ci-dessous et doivent être mises à jour régulièrement pour tenir compte de l'évolution des technologies et des normes ainsi que des travaux réalisés sur la base de la recommandation (UE) 2021/946, dont l'architecture et le cadre de référence:

1) aux attestations électroniques d'attributs qualifiées;

2) aux attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte;

3) à la liste des fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte;

4) au catalogue d'attributs et au catalogue de programmes d'attestation d'attributs visés aux points 1) et 2);

5) à la vérification des attributs par rapport aux sources authentiques ou via des intermédiaires désignés.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

1) «unité de portefeuille», une configuration unique d'une solution de portefeuille comprenant des instances de portefeuille, des applications cryptographiques sécurisées de portefeuille et des dispositifs cryptographiques sécurisés de portefeuille, fournie par un fournisseur de portefeuille à un utilisateur de portefeuille donné;

([6]) 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).

([7]) 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).

([8]) 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) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

2) «utilisateur de portefeuille», un utilisateur qui contrôle l'unité de portefeuille;

3) «catalogue d'attributs», un répertoire numérique d'attributs qui est tenu à jour et publié en ligne par la Commission;

4) «programme d'attestation d'attributs», un ensemble de règles applicables à un ou plusieurs types d'attestations électroniques d'attributs;

5) «type d'attestation électronique d'attributs», un groupe d'attestations électroniques d'attributs auquel sont attribués un nom spécifique et une description sémantique;

6) «catalogue de programmes d'attestation d'attributs», un répertoire numérique qui contient la liste des programmes d'attestation d'attributs enregistrés conformément au présent règlement et qui est tenu à jour [et publié en ligne] par la Commission;

7) «solution de portefeuille», une combinaison de logiciels, de matériel, de services, de paramètres et de configurations, y compris des instances de portefeuille, une ou plusieurs applications cryptographiques sécurisées de portefeuille et un ou plusieurs dispositifs cryptographiques sécurisés de portefeuille;

8) «instance de portefeuille», l'application installée et configurée sur l'appareil ou dans l'environnement d'un utilisateur de portefeuille, qui fait partie d'une unité de portefeuille et dont l'utilisateur de portefeuille se sert pour interagir avec l'unité de portefeuille;

9) «application cryptographique sécurisée de portefeuille», une application qui gère des actifs critiques en étant liée aux fonctions cryptographiques et non cryptographiques fournies par le dispositif cryptographique sécurisé de portefeuille et en utilisant ces fonctions;

10) «dispositif cryptographique sécurisé de portefeuille», un dispositif inviolable qui fournit un environnement lié à l'application cryptographique sécurisée de portefeuille et utilisé par celle-ci pour protéger les actifs critiques et fournir des fonctions cryptographiques pour l'exécution sécurisée d'opérations critiques;

11) «fournisseur de portefeuille», une personne physique ou morale qui fournit des solutions de portefeuille;

12) «actifs critiques», les actifs se trouvant à l'intérieur d'une unité de portefeuille ou en rapport avec celle-ci et dont l'importance est tellement exceptionnelle que la capacité de se fier à l'unité de portefeuille serait très sérieusement affaiblie si leur disponibilité, leur confidentialité ou leur intégrité étaient compromises;

13) «propriétaire d'un programme d'attestation d'attributs», une entité chargée de mettre en place et de tenir à jour un programme d'attestation d'attributs.

Article 3

Délivrance des attestations électroniques d'attributs qualifiées et des attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte

1. Les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte respectent les normes de références et spécifications énumérées à l'annexe I et veillent à ce que les attestations électroniques d'attributs qu'ils délivrent soient conformes aux spécifications techniques énoncées à l'annexe II.

2. Lorsque les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte délivrent des attestations électroniques d'attributs qui sont couvertes par des programmes enregistrés dans le catalogue de programmes d'attestation d'attributs, ils se conforment aux exigences du programme d'attestation d'attributs correspondant. Les règles et procédures établies par les entités délivrant des attestations pour assurer la conformité avec les exigences des programmes d'attestation d'attributs sont prises en compte dans l'évaluation de la conformité prévue par le règlement (UE) n° 910/2014.

Article 4

Révocation des attestations électroniques d'attributs qualifiées et des attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte

1. Les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte disposent de règles écrites et accessibles au public concernant la gestion du statut de validité ou de révocation. Ces règles devraient inclure, le cas échéant, les conditions dans lesquelles les attestations électroniques d'attributs peuvent être révoquées sans délai et les mesures permettant d'assurer la disponibilité des informations relatives au statut de validité.

2. Les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte sont les seules entités capables de révoquer les attestations électroniques d'attributs qu'ils délivrent.

3. Lorsque la période de validité des attestations fournies par les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte est supérieure à 24 heures, les fournisseurs de ces attestations les révoquent au moins dans les cas suivants:

a) à la demande explicite de la personne à laquelle l'attestation électronique d'attributs a été délivrée ou, le cas échéant, de la personne à laquelle l'attestation se rapporte;

b) lorsque le fournisseur sait que la sécurité ou la fiabilité des attestations électroniques d'attributs qualifiées ou des attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte a été compromise;

c) dans d'autres situations, couvertes par le droit de l'Union ou le droit national, ou définies par les fournisseurs dans leurs règles visées au paragraphe 1.

4. Les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte mettent en place des techniques de révocation et des méthodes de gestion des révocations qui garantissent la protection de la vie privée et empêchent l'associabilité et la traçabilité.

5. Les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte mettent à la disposition des parties utilisatrices des informations sur le statut de validité ou de révocation des attestations électroniques d'attributs qu'ils ont délivrées d'une manière qui garantit l'intégrité et l'authenticité de ces informations.

Article 5

Notification des organismes du secteur public

1. Les États membres transmettent au moins les informations mentionnées à l'annexe III concernant les organismes du secteur public visés à l'article 45 *septies*, paragraphe 3, du règlement (UE) n° 910/2014 au moyen d'un système de notification électronique sécurisé fourni par la Commission.

2. Les États membres notifient toute modification apportée aux informations transmises.

3. Les États membres transmettent les notifications au moins en anglais. Ils ne sont pas tenus de faire traduire les documents à l'appui des notifications si cela engendre une charge administrative ou financière déraisonnable.

4. La Commission peut, au besoin, demander aux États membres de fournir des informations complémentaires.

Article 6

Publication de la liste des organismes du secteur public

1. La Commission établit, tient à jour et publie une liste des fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte à partir des informations notifiées par les États membres au titre de l'article 5.

2. La Commission veille à ce que la liste visée au paragraphe 1 soit accessible:

a) sous une forme portant une signature électronique ou un cachet électronique adaptée au traitement automatisé et sur un site web lisible par l'être humain;

b) sans qu'il soit nécessaire de s'inscrire ou de s'authentifier;

c) en utilisant uniquement le protocole «sécurité de la couche de transport» le plus récent.

3. La Commission publie, par l'intermédiaire d'un canal sécurisé et sans retard injustifié:

a) les spécifications techniques de la liste;

b) l'adresse URL à laquelle la liste est publiée;

c) les certificats à utiliser pour vérifier la signature électronique ou le cachet électronique apposé(e) sur la liste;

d) les informations relatives aux mécanismes utilisés pour valider les modifications apportées ultérieurement à l'adresse ou aux certificats mentionnés aux points b) et c).

Article 7

Création et mise à jour du catalogue d'attributs

1. La Commission établit et publie un catalogue d'attributs et met en place un système sécurisé permettant de demander l'inclusion ou la modification d'attributs dans ce catalogue.

2. La Commission évalue les demandes d'inclusion ou de modification d'un attribut dans le catalogue d'attributs faites au moyen du système visé au paragraphe 1 en tenant compte de tout éventuel avis donné par le groupe de coopération. Dans le cadre de cette évaluation, la Commission examine si l'inclusion de l'attribut contribue à former une base commune permettant des interactions électroniques sécurisées et respectueuses de la vie privée entre les citoyens, les entreprises et les pouvoirs publics et s'il contribue à l'interopérabilité. Le cas échéant, la Commission tient également compte de la réglementation sectorielle.

3. Les États membres demandent que des attributs énumérés à l'annexe VI du règlement (UE) n° 910/2014 soient inclus dans le catalogue d'attributs lorsque la vérification de ces attributs par des prestataires de services de confiance qualifiés repose sur des sources authentiques.

4. En outre, les États membres peuvent demander l'inclusion d'attributs qui ne sont pas énumérés à l'annexe VI dans le catalogue d'attributs lorsque ces attributs reposent sur des sources authentiques du secteur public. Les entités privées qui sont considérées comme étant une source première d'informations ou reconnues comme authentiques conformément au droit de l'Union ou au droit national, y compris les pratiques administratives, peuvent demander l'inclusion d'attributs qui ne sont pas énumérés à l'annexe VI dans le catalogue d'attributs, à condition que l'entité à l'origine de la demande soit responsable de ces attributs.

5. La demande d'inclusion ou de modification d'un attribut dans le catalogue contient au moins les informations suivantes:

a) l'identification de l'entité à l'origine de la demande;

b) le cas échéant, une référence à la disposition du droit de l'Union, du droit national ou à la pratique administrative en vertu de laquelle l'entité à l'origine de la demande est considérée comme étant une source première d'informations ou reconnue comme une source authentique;

c) si la demande porte sur un attribut déjà enregistré dans le catalogue ou sur un nouvel attribut;

d) un espace de noms pour l'identifiant des attributs, dont la valeur est unique au sein du catalogue d'attributs;

e) l'identifiant de l'attribut, unique au sein de l'espace de noms, et la version de l'attribut;

f) une description sémantique de l'attribut;

g) le type de données de l'attribut;

h) le point de vérification de l'attribut au niveau national ou un lien renvoyant vers une description des modalités d'ouverture des demandes de vérification.

6. La demande d'inclusion ou de modification d'un attribut est signée ou cachetée par le demandeur au moyen d'une signature électronique qualifiée ou d'un cachet électronique qualifié, ou d'une signature électronique avancée ou d'un cachet électronique avancé reposant sur un certificat qualifié.

7. Après avoir effectué l'évaluation visée au paragraphe 2 et vérifié que les informations fournies dans la demande d'inclusion ou de modification d'un attribut comprennent tous les éléments énumérés au paragraphe 5, la Commission peut inclure ou modifier l'attribut faisant l'objet de la demande dans le catalogue d'attributs.

8. Le catalogue d'attributs, portant le cachet de la Commission, est accessible au public gratuitement, par l'intermédiaire d'un canal sécurisé, sans identification ou authentification préalables, et publié sous une forme lisible à la fois par la machine et par l'être humain. Le catalogue intègre également une fonction de recherche.

9. La Commission publie les spécifications techniques qu'elle utilise pour le catalogue d'attributs.

10. La Commission émet un identifiant unique pour chaque attribut enregistré.

Article 8

Création et mise à jour du catalogue de programmes d'attestation d'attributs

1. La Commission établit et publie un catalogue de programmes d'attestation d'attributs et met en place un système sécurisé permettant de demander l'inclusion ou la modification de programmes d'attestation d'attributs dans ce catalogue.

2. La Commission évalue les demandes d'inclusion ou de modification de programmes d'attestation d'attributs dans le catalogue de programmes d'attestation d'attributs en tenant compte de tout éventuel avis donné par le groupe de coopération. Dans le cadre de cette évaluation, la Commission examine si le programme contribue à former une base commune favorisant des interactions électroniques sécurisées et respectueuses de la vie privée entre les citoyens, les entreprises et les pouvoirs publics et si elle contribue à l'interopérabilité. Le cas échéant, la Commission tient également compte de la réglementation sectorielle.

3. Les propriétaires d'un programme d'attestation d'attributs peuvent demander l'ajout de programmes au catalogue de programmes. Une demande d'inclusion ou de modification d'un programme dans le catalogue de programmes d'attestation d'attributs contient au moins:

a) le nom du programme, choisi par le propriétaire du programme d'attestation d'attributs et unique au sein du catalogue de programmes d'attestation d'attributs;

b) le nom et les coordonnées du propriétaire du programme d'attestation d'attributs;

c) le statut et la version du programme;

d) une référence aux lois, normes ou lignes directrices spécifiques desquelles dépendent la délivrance, la validation ou l'utilisation d'une attestation électronique d'attributs couverte par le programme;

e) le ou les formats de l'attestation électronique d'attributs couverte par le programme;

f) un ou plusieurs espaces de noms, identifiants d'attributs, descriptions sémantiques et types de données pour chaque attribut faisant partie d'une attestation électronique d'attributs couverte par le programme, soit par référence à un attribut figurant dans le catalogue d'attributs visé à l'article 7, soit par référence à un attribut défini de manière similaire dans le cadre du programme;

g) une description du modèle de confiance et des mécanismes de gouvernance appliqués dans le cadre du programme, y compris des mécanismes de révocation;

h) toute exigence concernant les fournisseurs d'attestations électroniques d'attributs ou les sources d'information sur lesquelles ces fournisseurs s'appuient lorsqu'ils délivrent des attestations électroniques d'attributs, y compris toute source authentique, le cas échéant;

i) une déclaration indiquant si les attestations électroniques d'attributs couvertes par le programme doivent être délivrées sous la forme d'attestations électroniques d'attributs qualifiées, d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte, ou les deux.

4. Les programmes qui font l'objet d'une demande d'inclusion dans le catalogue ne contiennent que des attributs identifiables au moyen d'identifiants uniques. La demande d'inclusion ou de modification d'un programme d'attestation d'attributs est signée ou cachetée par le demandeur au moyen d'une signature électronique qualifiée ou d'un cachet électronique qualifié, ou d'une signature électronique avancée ou d'un cachet électronique avancé reposant sur un certificat qualifié.

5. Après avoir effectué l'évaluation visée au paragraphe 2 et vérifié que les informations fournies dans la demande d'inclusion ou de modification d'un programme d'attestation d'attributs comprennent tous les éléments énumérés aux paragraphes 3 et 4, la Commission peut inclure ou modifier le programme faisant l'objet de la demande dans le catalogue de programmes d'attestation d'attributs.

6. Le catalogue de programmes d'attestation d'attributs, portant le cachet de la Commission, est accessible au public gratuitement, par l'intermédiaire d'un canal sécurisé, sans identification ou authentification préalables, et est lisible par la machine et par l'être humain. Le catalogue intègre également une fonction de recherche et se présente dans un format qui garantit l'intégrité et l'authenticité.

7. La Commission publie les spécifications techniques qu'elle utilise pour le catalogue de programmes d'attestation d'attributs.

8. La Commission émet un identifiant unique pour chaque programme d'attestation d'attributs enregistré.

Article 9

Vérification des attributs par rapport aux sources authentiques ou via des intermédiaires désignés

1. Pour permettre la vérification électronique des attributs à la demande de l'utilisateur, telle que prévue à l'article 45 *sexies*, paragraphe 1, du règlement (UE) n° 910/2014, par des prestataires de services de confiance qualifiés délivrant des attestations électroniques d'attributs qualifiées, les États membres mettent en place des mécanismes permettant cette vérification et peuvent mettre à disposition des points de vérification uniques pour les attributs énumérés à l'annexe VI dudit règlement lorsque ces attributs reposent sur des sources authentiques du secteur public. Les États membres publient des informations relatives aux procédures d'ouverture des demandes de vérification et de réception des résultats de la vérification.

2. Le mécanisme de vérification fournit un point d'accès permettant aux prestataires de services de confiance qualifiés délivrant des attestations électroniques d'attributs qualifiées de demander, par voie électronique, la vérification des attributs visés à l'article 45 *sexies*, paragraphe 1, du règlement (UE) n° 910/2014 par rapport aux sources authentiques ou via des intermédiaires désignés reconnus au niveau national. Les attributs faisant l'objet de la vérification seront fournis au point de vérification par le prestataire de services de confiance qualifié à la demande de l'utilisateur. L'organisme du secteur public ou l'intermédiaire désigné communique, par l'intermédiaire du point de vérification, les résultats de la vérification aux prestataires de services de confiance qualifiés délivrant des attestations électroniques d'attributs qualifiées.

3. La demande de vérification contient les attributs et les données d'identification de la personne à laquelle se rapporte l'attribut dont le prestataire de services de confiance qualifié demande la vérification.

4. Le résultat de la vérification indique uniquement si l'attribut a été vérifié ou non et précise l'organisme du secteur public responsable de la source authentique ou, le cas échéant, l'organisme du secteur public désigné pour agir pour le compte de la source authentique ayant servi à la vérification de l'attribut.

5. Les États membres peuvent imposer des contrôles d'accès ou d'autres mécanismes de vérification qui garantissent l'intégrité, l'authenticité et la confidentialité afin d'établir que le demandeur est un prestataire de services de confiance qualifié et qu'il agit à la demande d'un utilisateur légitime. Les États membres peuvent également imposer des mécanismes de contrôle de l'utilisation des méthodes de vérification, lorsqu'ils le jugent approprié, en tenant compte de facteurs pertinents, par exemple du fait que les sources authentiques contiennent des données à caractère personnel de nature confidentielle ou sensible. Lorsque les États membres mettent en place de tels mécanismes de contrôle, ils publient des informations relatives à l'étendue de ces mécanismes dans le cadre des informations visées au paragraphe 1.

Article 10

Interopérabilité et réutilisation

1. Aux fins des articles 3 à 9, les États membres peuvent se référer aux services communs du système technique établi en vertu de l'article 14 du règlement (UE) 2018/1724 ainsi qu'aux composantes nationales qui y sont connectées, et les réutiliser.

2. Lorsqu'elle établit le système de notification sécurisé et la liste des organismes du secteur public visés aux articles 5 et 6 ainsi que les catalogues visés aux articles 7 et 8 du présent règlement, la Commission européenne se réfère aux services communs du système technique prévu par le règlement (UE) 2018/1724 et les réutilise, le cas échéant.

Article 11

Entrée en vigueur et application

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

Les articles 6 à 9 sont applicables à partir du 19 août 2026.

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

ANNEXE I

Liste des normes de référence et des spécifications mentionnées à l'article 3

Les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte délivrent leurs attestations à des personnes physiques ou morales conformément aux spécifications applicables aux prestataires de services de confiance définies dans la norme ETSI EN 319 401 v3.1.1 (2024-06) («ETSI EN 319 401»).

ANNEXE II

Spécifications techniques relatives à la délivrance des attestations électroniques d'attributs qualifiées et des attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte mentionnées à l'article 3

1) Les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte délivrent leurs attestations dans un format conforme à l'une des normes énumérées à l'annexe II du règlement d'exécution (UE) 2024/2979 de la Commission ([1]).

2) Lorsqu'ils délivrent des attestations à des personnes physiques ou morales, les fournisseurs d'attestations électroniques d'attributs qualifiées et les fournisseurs d'attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte doivent:

   a) le cas échéant, vérifier que le demandeur de l'attestation a le droit d'agir pour le compte de la personne à laquelle l'attestation se rapporte;

   b) le cas échéant, vérifier l'identité de la source authentique utilisée comme source pour les attributs inclus dans l'attestation;

   c) traiter uniquement le jeu d'attributs minimal nécessaire à la délivrance et à la gestion de l'attestation.

3) En outre, lorsque l'attestation est délivrée à un portefeuille européen d'identité numérique, le fournisseur de l'attestation doit:

   a) s'authentifier auprès de l'unité de portefeuille;

   b) vérifier que l'unité de portefeuille n'est ni révoquée, ni suspendue.

([1]) Règlement d'exécution (UE) 2024/2979 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne l'intégrité et les fonctionnalités essentielles des portefeuilles européens d'identité numérique (JO L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

ANNEXE III

Notifications visées à l'article 5

Les États membres notifient à la Commission au moins les informations suivantes:

1) le nom de l'organisme du secteur public et, le cas échéant, son numéro d'immatriculation tels qu'ils figurent dans les registres officiels; l'État membre dans lequel l'organisme du secteur public est établi; la disposition du droit de l'Union ou du droit national en vertu de laquelle l'organisme du secteur public est établi comme étant le responsable de la source authentique sur la base de laquelle l'attestation électronique d'attributs est délivrée ou est désigné pour agir pour le compte de l'organisme du secteur public responsable de la source authentique;

2) l'adresse électronique et le numéro de téléphone de l'organisme du secteur public;

3) l'adresse URL de la page web contenant des informations supplémentaires sur l'organisme du secteur public;

4) le rapport d'évaluation de la conformité prévu à l'article 45 *septies*, paragraphe 3, du règlement (UE) nº 910/2014.

Journal officiel
de l'Union européenne

FR
Série L

2025/1570

30.7.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/1570 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 notification des informations relatives aux dispositifs de création de signature électronique qualifiés certifiés et aux dispositifs de création de cachet électronique qualifiés certifiés

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 31, paragraphe 3, et son article 39, paragraphe 3,

considérant ce qui suit:

(1) Afin d'établir une source d'information transparente et fiable sur les dispositifs de création de signature électronique qualifiés et sur les dispositifs de création de cachet électronique qualifiés qui ont été certifiés, ou qui ne le sont plus, par les organismes de certification visés à l'article 30, paragraphe 1, du règlement (UE) nº 910/2014, les États membres doivent notifier les informations pertinentes à la Commission, au moyen d'un canal électronique sécurisé mis à disposition par la Commission.

(2) Afin de laisser suffisamment de temps à la Commission pour adapter le canal existant pour les notifications d'informations en ce qui concerne le statut de certification des dispositifs de création de signature électronique qualifiés et des dispositifs de création de cachet électronique qualifiés, le présent règlement devrait s'appliquer à partir de 3 mois à compter de son entrée en vigueur.

(3) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([2]) et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([3]) s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du présent règlement.

(4) 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 ([4]) et a rendu son avis le 6 juin 2025.

(5) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) nº 910/2014,

([1]) JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) 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).

([3]) 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).

([4]) 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) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

1. La notification visée à l'article 31, paragraphe 1, du règlement (UE) n° 910/2014 contient au moins les informations visées à l'annexe du présent règlement et est effectuée sous forme électronique par l'intermédiaire d'un canal électronique sécurisé mis à disposition par la Commission.

2. En cas de modification des informations communiquées après la soumission initiale, y compris des modifications du statut de certification des dispositifs de création de signature électronique qualifiés et des dispositifs de création de cachet électronique qualifiés, les États membres transmettent les informations mises à jour avec les documents d'accompagnement pertinents par le canal visé au paragraphe 1.

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 décembre 2025.

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

ANNEXE

Informations à communiquer par les États membres conformément à l'article 31, paragraphe 1

1. L'identification du dispositif de création de signature électronique qualifié ou du dispositif de création de cachet électronique qualifié, tel que couvert par la notification de la certification ou de l'annulation de la certification et précisé au moyen des éléments suivants:

   a) la dénomination du produit;

   b) la référence au composant logiciel configuré, y compris la version pertinente;

   c) la référence au composant matériel configuré, y compris la version pertinente;

   d) la version;

2. L'identité de l'organisme qui a demandé la certification;

3. La description du dispositif de création de signature électronique qualifié ou du dispositif de création de cachet électronique qualifié, y compris:

   a) s'il s'agit d'un dispositif de création de signature électronique qualifié et/ou d'un dispositif de création de cachet électronique qualifié;

   b) à laquelle des catégories suivantes appartient le dispositif:

      — dispositifs dans lesquels les données de création de signature électronique ou les données de création de cachet électronique sont conservées dans un environnement entièrement (mais pas nécessairement exclusivement) géré par l'utilisateur,

      — dispositifs dans lesquels un prestataire de services de confiance qualifié gère les données de création de signature électronique ou les données de création de cachet électronique pour le compte d'un signataire ou d'un créateur de cachet;

4. Le certificat de conformité du dispositif aux exigences de l'annexe II du règlement (UE) n° 910/2014;

5. Une référence au rapport de certification délivré conformément à l'article 30 du règlement (UE) n° 910/2014, qui ne doit pas changer au moins pendant la période de validité du certificat de conformité;

6. L'identité de l'entité de délivrance du rapport de certification, y compris une référence appropriée à sa qualification en tant qu'organisme de certification désigné par un État membre conformément à l'article 30, paragraphe 1, du règlement (UE) n° 910/2014 et en tant qu'organisme conforme pour la certification de ces dispositifs conformément à l'article 30, paragraphe 3, dudit règlement;

7. Un localisateur uniforme de ressources (URL) d'une localisation à partir de laquelle le rapport de certification est accessible gratuitement au public;

8. La date effective de début de la certification;

9. Le statut de la certification;

10. La date d'expiration de la certification;

11. S'il est prévu de ne pas poursuivre la certification après la certification actuelle pour la configuration actuelle des dispositifs de création de signature électronique qualifiés ou des dispositifs de création de cachet électronique qualifiés;

12. Les coordonnées de l'organisme désigné;

13. Si la méthode de certification est conforme ou non à l'article 30, paragraphe 3, premier alinéa, point a) ou b), du règlement (UE) nº 910/2014 et, le cas échéant, la référence et l'URL des autres procédures qui ont été notifiées à la Commission conformément à l'article 30, paragraphe 3, premier alinéa, point b), dudit règlement;

14. Tous les rapports de certification connexes établis conformément aux actes d'exécution adoptés en vertu de l'article 30, paragraphe 3, deuxième alinéa, du règlement (UE) nº 910/2014, y compris:

    a) une référence à chaque rapport de certification;

    b) l'identification de l'entité de délivrance de chaque rapport de certification;

    c) une URL vers une localisation à partir de laquelle chaque rapport de certification est accessible gratuitement au public;

    d) la date de délivrance de chaque rapport de certification;

    e) lorsqu'elle est accessible au public, une version de la cible de sécurité correspondante décrivant le dispositif, ou tout composant de celui-ci, faisant l'objet de l'évaluation de la certification couverte par le rapport de certification.

Journal officiel
de l'Union européenne

FR
Série L

2025/1571

30.7.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/1571 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 formats et procédures applicables aux rapports annuels des organes de contrôle

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 46 *bis*, paragraphe 7, et son article 46 *ter*, paragraphe 7,

considérant ce qui suit:

(1) Les organes de contrôle des portefeuilles européens d'identité numérique désignés en vertu de l'article 46 *bis*, paragraphe 1, du règlement (UE) nº 910/2014 et les organes de contrôle des services de confiance désignés en vertu de l'article 46 *ter*, paragraphe 1, dudit règlement (ci-après les «organes de contrôle») doivent fournir à la Commission des informations pertinentes sur leurs activités de contrôle conformément à l'article 46 *bis*, paragraphe 6, et à l'article 46 *ter*, paragraphe 6, dudit règlement.

(2) Afin de mettre en place une source d'informations transparente et fiable concernant les activités de contrôle des organes de contrôle, de veiller à ce que les échanges de données avec la Commission soient sûrs et vérifiables et de réduire la complexité administrative, les organes de contrôle devraient soumettre les rapports annuels dans un format spécifié, lisible par machine et adapté au traitement automatisé.

(3) Pour faciliter l'échange de bonnes pratiques entre les organes de contrôle et garantir la cohérence et l'efficacité des contrôles dans tous les États membres, il est essentiel que les rapports annuels des organes de contrôle contiennent des informations complètes et pertinentes. En particulier, les organes de contrôle devraient rendre compte de celles de leurs activités qui comportent des éléments susceptibles de renforcer la coopération, y compris, entre autres, donner des précisions sur les activités de contrôle menées et envisagées, les difficultés recensées, les inspections, les notifications d'atteinte à la sécurité importante ou de perte d'intégrité adressées par l'organe de contrôle aux autorités compétentes de l'État membre concerné en vertu de la directive (UE) 2022/2555 du Parlement européen et du Conseil ([2]), et l'assistance entre les organes de contrôle conformément aux articles 46 *quater* et 46 *quinquies* du règlement (UE) nº 910/2014. En outre, étant donné que ces informations figurant dans les rapports annuels doivent être mises à la disposition du Parlement européen et du Conseil conformément aux articles 46 *bis*, paragraphe 6, et 46 *ter*, paragraphe 6, du règlement (UE) nº 910/2014, les informations à fournir répondraient à l'objectif de transparence et d'accessibilité de l'information. Par conséquent, tous les organes de contrôle devraient communiquer les informations visées aux annexes I et II du présent règlement.

([1]) JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(4) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([3]) ainsi que, le cas échéant, le règlement (UE) 2018/1725 du Parlement européen et du Conseil ([4]) et la directive 2002/58/CE du Parlement européen et du Conseil ([5]) s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du présent règlement.

(5) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 et a rendu son avis le 28 mai 2025.

(6) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Format et procédures des rapports annuels

1. Les organes de contrôle soumettent à la Commission leurs rapports annuels visés à l'article 46 *bis*, paragraphe 6, et à l'article 46 *ter*, paragraphe 6, du règlement (UE) nº 910/2014, par l'intermédiaire d'un canal électronique sécurisé mis à disposition par la Commission.

2. Les organes de contrôle ne transmettent les informations dans leurs rapports annuels qu'une seule fois, en réutilisant, le cas échéant, les informations précédemment communiquées.

3. Les organes de contrôle des portefeuilles européens d'identité numérique visés à l'article 46 *bis*, paragraphe 1, du règlement (UE) nº 910/2014 veillent à ce que leurs rapports annuels contiennent au moins les informations visées à l'annexe I du présent règlement.

4. Les organes de contrôle des services de confiance visés à l'article 46 *ter*, paragraphe 1, du règlement (UE) nº 910/2014 veillent à ce que leurs rapports annuels contiennent au moins les informations visées à l'annexe II du présent règlement.

([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]) 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) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([5]) 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).

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 29 juillet 2025.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE I

Informations à inclure dans les rapports annuels des organes de contrôle des portefeuilles européens d'identité numérique

Les rapports annuels des organes de contrôle des portefeuilles européens d'identité numérique contiennent au moins les informations suivantes:

1) le nom, l'adresse et les coordonnées de l'organe de contrôle qui soumet le rapport annuel;

2) lorsque plusieurs organes de contrôle ont été désignés conformément à l'article 46 *bis*, paragraphe 1, du règlement (UE) n° 910/2014, le champ d'application des activités de contrôle de l'organe de contrôle qui soumet le rapport annuel;

3) une description de l'organisation, de la structure, des ressources et des capacités de l'organe de contrôle;

4) une description des activités de contrôle ex post et ex ante menées pour chaque fournisseur de portefeuille au cours de l'année civile précédente conformément à l'article 46 *bis*, paragraphe 3, point a), y compris les cas d'infractions présumées ou potentielles au règlement (UE) n° 910/2014 et un résumé des principaux défis recensés;

5) un résumé des inspections sur place et des activités de contrôle hors site menées par l'organe de contrôle, comprenant au moins les informations suivantes:

   a) l'identification du ou des fournisseurs de portefeuille;

   b) la ou les solutions de portefeuille affectées;

   c) un résumé du résultat;

   d) toute mesure imposée;

   e) toute action entreprise par l'organe de contrôle;

6) une description des activités de contrôle ex post menées conformément à l'article 46 *bis*, paragraphe 3, point b), du règlement (UE) n° 910/2014 et un résumé des principaux défis recensés;

7) une description des notifications d'atteinte à la sécurité importante ou de perte d'intégrité adressées par l'organe de contrôle aux autorités compétentes de l'État membre concerné, désignées ou établies en vertu de l'article 8, paragraphe 1, de la directive (UE) 2022/2555, aux points de contact uniques de l'État membre concerné, désignés ou établis en vertu de l'article 8, paragraphe 3, de la directive (UE) 2022/2555, aux points de contact uniques de l'autre ou des autres États membres concernés, désignés en vertu de l'article 46 *quater*, paragraphe 1, du règlement (UE) n° 910/2014, ou au public;

8) des informations sur les demandes adressées aux fournisseurs de portefeuilles en vue de remédier à tout manquement aux exigences énoncées dans le règlement (UE) n° 910/2014;

9) une description des cas dans lesquels l'enregistrement des parties utilisatrices dans le mécanisme visé à l'article 5 *ter*, paragraphe 7, du règlement (UE) n° 910/2014 a été annulé pour des raisons d'utilisation illégale ou frauduleuse du portefeuille européen d'identité numérique;

10) une description de toute coopération ou assistance avec d'autres organes de contrôle établis dans d'autres États membres, conformément aux articles 46 *quater* et 46 *sexies* du règlement (UE) n° 910/2014, et une vue d'ensemble des résultats de cette coopération;

11) la fréquence et la nature de la coopération avec les autorités de contrôle compétentes instituée en vertu de l'article 51 du règlement (UE) 2016/679;

12) un aperçu des activités de contrôle et des priorités sur lesquelles l'organe de contrôle entend se concentrer au cours de l'année suivante.

ANNEXE II

Informations à inclure dans les rapports annuels des organes de contrôle des services de confiance

Les rapports annuels des organes de contrôle contiennent au moins les informations suivantes:

1) le nom, l'adresse et les coordonnées de l'organe de contrôle qui soumet le rapport annuel;

2) lorsque plusieurs organes de contrôle ont été désignés conformément à l'article 46 *ter*, paragraphe 1, du règlement (UE) n° 910/2014, le champ d'application des activités de contrôle de l'organe de contrôle qui soumet le rapport annuel;

3) une description de l'organisation, de la structure, des ressources et des capacités de l'organe de contrôle qui soumet le rapport annuel;

4) une description des activités de contrôle exercées en vertu de l'article 46 *ter*, paragraphe 3, points a) et b), au cours de l'année civile concernée, à l'égard des prestataires de services de confiance non qualifiés et qualifiés établis sur le territoire de l'État membre qui a procédé à la désignation et des services de confiance qu'ils fournissent, y compris les cas d'infractions présumées ou potentielles au règlement (UE) n° 910/2014, et un résumé des principaux défis recensés;

5) un résumé des inspections sur place et des activités de contrôle hors site menées par l'organe de contrôle qui soumet le rapport annuel, comprenant au moins les informations suivantes:

   a) l'identification du ou des prestataires de services de confiance qualifiés;

   b) le ou les services de confiance affectés;

   c) une description de l'activité de contrôle;

   d) un résumé du résultat;

   e) toute mesure imposée;

   f) toute action entreprise par l'organe de contrôle;

6) une description de toute mesure supplémentaire prise par l'organe de contrôle en vertu de l'article 46 *ter*, paragraphe 3, du règlement (UE) n° 910/2014;

7) une description des notifications d'atteinte à la sécurité importante ou de perte d'intégrité adressées par l'organe de contrôle qui soumet le rapport annuel aux autorités compétentes de l'État membre ou des États membres concernés, désignées ou établies en vertu de l'article 8, paragraphe 1, de la directive (UE) 2022/2555, aux points de contact uniques de l'État membre ou des États membres concernés, désignés ou établis en vertu de l'article 8, paragraphe 3, de la directive (UE) 2022/2555, aux points de contact uniques des autres États membres concernés, désignés en vertu de l'article 46 *quater*, paragraphe 1, du règlement (UE) n° 910/2014, ou au public;

8) une description du domaine de coopération avec d'autres organes de contrôle établis dans d'autres États membres et une description de l'assistance fournie conformément aux articles 46 *quater* et 46 *sexies* du règlement (UE) n° 910/2014, et une vue d'ensemble des résultats de cette coopération;

9) une description de la fréquence et de la nature de la coopération des organes de contrôle des services de confiance avec les autorités de contrôle compétentes établies en vertu de l'article 51 du règlement (UE) 2016/679, lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ont été enfreintes, et en cas d'atteintes à la sécurité dont il apparaît qu'elles constituent des violations de données à caractère personnel en ce qui concerne les prestataires de services de confiance et les services de confiance qu'ils fournissent;

10) un résumé du résultat de la vérification de l'existence et de l'application correcte de dispositions relatives aux plans d'arrêt d'activité, lorsqu'un prestataire de services de confiance qualifié contrôlé cesse ses activités, y compris une indication de la manière dont les informations restent accessibles conformément à l'article 24, paragraphe 2, point h), du règlement (UE) n° 910/2014;

11) une description de toute enquête suite à des plaintes introduites par les fournisseurs de navigateurs web sur lesquelles ils ont enquêté au cours de la période de référence conformément à l'article 45 *bis* du règlement (UE) n° 910/2014 et sur toute autre mesure consécutive prise dans ce contexte;

12) une description des activités liées aux listes de confiance visées à l'article 22 du règlement (UE) nº 910/2014, y compris des mises à jour notables à la suite d'activités de contrôle, d'une expérience appropriée ou de problèmes de conformité avec la décision d'exécution (UE) 2015/1505 de la Commission [1], en particulier en ce qui concerne les exigences en matière de disponibilité;

13) des informations sur les systèmes nationaux d'accréditation des organismes d'évaluation de la conformité, les systèmes nationaux d'évaluation de la conformité ou les orientations connexes aux systèmes d'évaluation de la conformité, ou des informations sur les initiatives connexes;

14) une description, le cas échéant, de toute infrastructure de confiance établie, gérée et actualisée par un organe de contrôle à la demande d'un État membre et conformément au droit national.

[1] Décision d'exécution (UE) 2015/1505 de la Commission du 8 septembre 2015 établissant les spécifications techniques et les formats relatifs aux listes de confiance visées à l'article 22, paragraphe 5, du règlement (UE) nº 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (JO L 235 du 9.9.2015, p. 26, ELI: http://data.europa.eu/eli/dec_impl/2015/1505/oj).

Journal officiel
de l'Union européenne

FR
Série L

2025/1572

30.7.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/1572 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 formats et les procédures de notification d'intention et de vérification applicables au lancement de services de confiance 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 21, paragraphe 4,

considérant ce qui suit:

1) Lorsque des prestataires de services de confiance ont l'intention de commencer à fournir un service de confiance qualifié, il leur incombe de notifier à l'organe de contrôle leur intention accompagnée d'un rapport d'évaluation de la conformité délivré par un organisme d'évaluation de la conformité confirmant le respect des exigences fixées par le règlement nº 910/2014. Il appartient à l'organe de contrôle de vérifier si le prestataire de services de confiance et les services de confiance qu'il fournit respectent les exigences énoncées dans ledit règlement. Si l'organe de contrôle conclut que le prestataire de services de confiance et les services de confiance qu'il fournit respectent ces exigences, il lui incombe d'accorder le statut qualifié au prestataire de services de confiance et aux services de confiance que ce dernier fournit. À cette fin, les organes de contrôle devraient publier des informations sur la manière dont les prestataires de services de confiance sont censés notifier leur intention de devenir prestataires de services de confiance qualifiés. Afin de garantir que les prestataires de services de confiance qualifiés opèrent dans les mêmes conditions partout dans l'Union, il est nécessaire que les vérifications des organes de contrôle portent sur le même type d'informations concernant les prestataires de services de confiance et qu'elles soient effectuées de la même manière.

2) Les organes de contrôle devraient garantir la transparence quant à la manière dont ils traitent les informations que les prestataires de services de confiance font figurer dans leurs notifications. Les organes de contrôle devraient donc rédiger et publier une description de la manière dont ils vérifient si le prestataire de services de confiance respecte les exigences applicables.

3) Le règlement devrait s'appliquer 12 mois après son entrée en vigueur afin que les États membres disposent d'une période transitoire suffisante pour leur permettre de se conformer aux exigences du présent règlement en procédant aux adaptations nécessaires en ce qui concerne les notifications aux organes de contrôle. Ces adaptations peuvent comprendre la mise à jour des législations nationales, des lignes directrices organisationnelles et des systèmes d'information nationaux.

([1]) JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

4) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([2]) et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([3]) s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du présent règlement.

5) 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 ([4]) et a rendu son avis le 6 juin 2025.

6) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Méthode de vérification

1. Les organes de contrôle établissent une méthode pour vérifier que les prestataires de services de confiance ayant notifié leur intention de commencer à fournir un service de confiance qualifié respectent les exigences énoncées dans le règlement (UE) nº 910/2014 et à l'article 21, paragraphe 2, de la directive (UE) 2022/2555 du Parlement européen et du Conseil ([5]).

2. La méthode de vérification comprend des procédures et des processus permettant d'associer les autorités compétentes désignées ou établies en vertu de l'article 8, paragraphe 1, de la directive (UE) 2022/2555, qui mènent des actions de supervision afin de vérifier le respect, par le prestataire de services de confiance, des exigences énoncées à l'article 21 de la directive (UE) 2022/2555.

Article 2

Transparence

Les organes de contrôle publient les informations suivantes:

1) les coordonnées de l'organe de contrôle;

2) les canaux de communication à utiliser lorsque les prestataires de services de confiance notifient leur intention de commencer à fournir un service de confiance qualifié;

3) la liste des documents que les prestataires de services de confiance doivent fournir dans le cadre d'une notification de l'intention de commencer à fournir un service de confiance qualifié;

4) les procédures de traitement des réclamations relatives au processus permettant de vérifier que les prestataires de services de confiance ayant notifié leur intention de commencer à fournir un service de confiance qualifié respectent les exigences énoncées dans le règlement (UE) nº 910/2014 et à l'article 21, paragraphe 2, de la directive (UE) 2022/2555;

5) une description générale de la méthode mentionnée à l'article 1er.

([2]) 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).

([3]) 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).

([4]) 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) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([5]) Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

Article 3

Notifications des prestataires de services de confiance

Les prestataires de services de confiance fournissent au moins les informations suivantes dans leurs notifications d'intention de commencer à fournir un service de confiance qualifié:

1) lorsque le prestataire de services de confiance est une personne morale, son nom et, le cas échéant, un numéro d'enregistrement, le nom de l'État membre dans lequel il est établi et le nom de la ou des personnes qui signent ou soumettent la notification au nom de la personne morale;

2) lorsque le prestataire de services de confiance est une personne physique, son nom et son numéro d'identification personnel et, à défaut, sa date de naissance ainsi que le type et le numéro de son document d'identité;

3) le numéro de téléphone, l'adresse électronique et l'adresse postale du prestataire de services de confiance;

4) les identifiants uniformes de ressources (URI) permettant aux utilisateurs d'obtenir des informations supplémentaires concernant ce prestataire de services de confiance, y compris les déclarations et politiques en matière de pratiques, les conditions générales et les politiques de service à la clientèle qui s'appliquent au service de confiance notifié;

5) l'analyse des risques sous-tendant les mesures visées à l'article 24, paragraphe 2, point f *bis*), du règlement (UE) nº 910/2014 et l'analyse des risques sous-tendant les mesures visées à l'article 21 de la directive (UE) 2022/2555;

6) chaque service de confiance qualifié que le prestataire de services de confiance a l'intention de commencer à fournir;

7) pour chaque service de confiance que le prestataire de services de confiance a l'intention de commencer à fournir en tant que service de confiance qualifié:

   — un ou plusieurs identifiants et, le cas échéant, certificats du service de confiance, à inclure dans la liste nationale de confiance conformément aux actes d'exécution adoptés en vertu de l'article 22, paragraphe 5, du règlement (UE) nº 910/2014,

   — la date prévue pour le début de la fourniture du service de confiance,

   — le ou les rapports d'évaluation de la conformité du service de confiance et les coordonnées de l'organisme d'évaluation de la conformité,

   — le cas échéant, les rapports techniques étayant le rapport d'évaluation de la conformité;

8) le plan d'arrêt d'activité mentionné à l'article 24, paragraphe 2, point i), du règlement (UE) nº 910/2014.

Article 4

Vérifications par les organes de contrôle

1. Afin de déterminer si le prestataire de services de confiance et le service de confiance qualifié que celui-ci a l'intention de fournir respectent les exigences du règlement (UE) nº 910/2014 et de l'article 21 de la directive (UE) 2022/2555, les organes de contrôle analysent les informations fournies par le prestataire de services de confiance et peuvent, en sus des éventuelles mesures décrites dans la méthode établie conformément à l'article 1er, effectuer des vérifications sur place, et mener des entretiens avec des représentants du prestataire de services de confiance et de l'organisme d'évaluation de la conformité.

2. Les organes de contrôle vérifient au moins les éléments suivants:

a) le rapport d'évaluation de la conformité présenté contient suffisamment d'éléments démontrant que le prestataire de services de confiance et le service de confiance qualifié qu'il a l'intention de fournir respectent les exigences énoncées dans le règlement (UE) nº 910/2014 et à l'article 21 de la directive (UE) 2022/2555;

b) le rapport d'évaluation de la conformité soumis satisfait aux exigences énoncées dans les actes d'exécution adoptés en vertu de l'article 20, paragraphe 4, du règlement (UE) nº 910/2014;

c) toute information contenue dans le rapport d'évaluation de la conformité présenté indiquant que les exigences du règlement (UE) nº 910/2014 ne sont pas respectées;

d) toute information supplémentaire jugée nécessaire pour vérifier le respect des exigences énoncées dans le règlement (UE) nº 910/2014 et à l'article 21 de la directive (UE) 2022/2555.

Article 5

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 2026.

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

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.

Journal officiel
de l'Union européenne

FR
Série L

2025/1942

30.9.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/1942 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 services de validation qualifiés des signatures électroniques qualifiées et les services de validation qualifiés des cachets 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 33, paragraphe 2, et son article 40,

considérant ce qui suit:

(1) Les services de validation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés garantissent l'intégrité, l'authenticité et la correction du processus et des résultats de la validation, respectivement, des signatures électroniques qualifiées et des cachets électroniques qualifiés. Ces services de confiance 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.

(2) La présomption de conformité prévue à l'article 33, paragraphe 2, et à l'article 40 du règlement (UE) nº 910/2014 ne devrait s'appliquer que lorsque les services de validation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés sont conformes aux normes techniques 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 des service de confiance qualifiés, ainsi que la capacité de vérifier le statut qualifié et la validité technique des signatures électroniques qualifiées et des cachets électroniques qualifiés.

(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, 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).

(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 aux activités de traitement de données à caractère personnel au titre du présent règlement.

(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 institué par l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Normes et spécifications de référence

Les normes de référence et les spécifications visées à l'article 33, paragraphe 2, et à l'article 40 du règlement (UE) nº 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 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) nº 45/2001 et la décision nº 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 de validation qualifiés des signatures électroniques qualifiées et les services de validation qualifiés des cachets électroniques qualifiés

Les normes ETSI TS 119 441 V1.2.1 (2023-10) ([1]) («ETSI TS 119 441») et ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) («ETSI TS 119 172-4») s'appliquent moyennant les adaptations suivantes:

1. Pour l'ETSI TS 119 441

   1) 2.1 Références normatives

   — [1] ETSI TS 119 101 V1.1.1 (2016-03) Signatures électroniques et infrastructures (ESI) – Exigences en matière de politique et de sécurité pour les applications de création et de validation de signatures.

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

   — [3] ETSI EN 319 102-1 V1.4.1 (2024-06) Signatures électroniques et infrastructures (ESI) – Procédures de création et de validation des signatures numériques AdES – Partie 1: création et validation.

   — [4] 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.

   — [5] vide

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

   — [7] Règlement d'exécution (UE) 2024/482 de la Commission ([3]) 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] ETSI TS 119 172-4 V1.1.1 (2021-05) Signatures électroniques et infrastructures (ESI) – Politiques de signature – Partie 4: (politique de validation des) règles d'applicabilité des signatures pour les signatures électroniques qualifiées et les cachets électroniques qualifiés européens utilisant des listes de confiance.

   — [9] ETSI TS 119 102-2 V1.4.1 (2023-06) Signatures électroniques et infrastructures (ESI) – Procédures de création et de validation des signatures numériques AdES – Partie 2: rapport de validation des signatures.

   — [10] 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) ([4]).

   — [11] Règlement d'exécution (UE) 2024/3144 de la Commission ([5]) modifiant le règlement d'exécution (UE) 2024/4822 en ce qui concerne les normes internationales applicables et rectifiant ledit règlement d'exécution.

   — [12] ETSI EN 319 411-1 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

([1]) ETSI TS 119 441 – Signatures électroniques et infrastructures (ESI) – Exigences en matière de politique applicables au prestataire de services de confiance fournissant des services de validation de signature, V1.2.1 (2023-10).

([2]) ETSI TS 119 172-4 – Signatures électroniques et infrastructures (ESI) – Politiques de signature – Partie 4: (politique de validation des) règles d'applicabilité des signatures pour les signatures électroniques qualifiées et les cachets électroniques qualifiés européens utilisant des listes de confiance, V1.1.1 (2021-05).

([3]) JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.

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

([5]) JO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 2.2 Références normatives

— [I.11] vide.

3) 3.3 Abréviations

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

4) 4.3.3 Processus

— REMARQUE 10: voir l'ETSI EN 319 102-1 [3] pour des orientations et l'ETSI TS 119 172-4 [8] pour des orientations supplémentaires aux fins de la signature qualifiée de l'UE ou du cachet qualifié de l'UE.

5) 6.1 Déclaration des pratiques du service de validation de signature

— OVR-6.1-02: la déclaration des pratiques du SVS doit être structurée comme prévu à l'annexe A.

— OVR-6.1-03: la déclaration des pratiques du SVS doit énumérer les politiques de SVS prises en charge ou y faire référence (par exemple au moyen d'OID) et les décrire brièvement.

6) 6.3 Politique en matière de sécurité de l'information

— OVR-6.3-02: la politique de sécurité doit documenter les contrôles de sécurité et de respect de la vie privée mis en œuvre pour protéger les données à caractère personnel.

7) 7.2 Ressources humaines

— OVR-7.2-02: le personnel des SVSP intervenant dans des rôles de confiance et, le cas échéant, leurs 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-7.2-03: la conformité au point OVR-7.2-02 implique des mises à jour régulières (au moins tous les 12 mois) portant sur les nouvelles menaces et les pratiques actuelles en matière de sécurité.

8) 7.5 Contrôles cryptographiques

— OVR-7.5-02 [CONDITIONNEL]: lorsque les rapports de validation sont signés, le certificat de signature public du SVSP correspondant à la clé de signature privée du SVSP doit être délivré par une autorité de certification digne de confiance, conformément à la politique de certification normalisée «NCP+» définie dans l'ETSI EN 319 411-1 [12]. Il devrait être délivré conformément à une politique de certification appropriée spécifiée dans l'ETSI EN 319 411-2 [i.17].

— OVR-7.5-03 [CONDITIONNEL]: lorsque les rapports de validation sont signés, la clé de signature privée du SVSP 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 [4] 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 [7] [11], et certifié au niveau EAL 4 ou supérieur; ou

c) jusqu'au 31.12.2030, FIPS PUB 140-3 [6] niveau 3.

Cette certification doit être faite par rapport à une cible de sécurité ou 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 autres mesures de sécurité non techniques.

Si le dispositif cryptographique sécurisé bénéficie d'une certification EUCC [7] [11], ce dispositif doit être configuré et utilisé conformément à cette certification.

— OVR-7.5-04: vide.

— OVR-7.5-06: toute exportation ou importation de clé de signature privée d'un SVSP 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.

9) 7.7 Sécurité de fonctionnement

— OVR-7.7-02: afin de garantir que les systèmes sur lesquels l'application est développée appliquent des mesures de sécurité appropriées et s'adaptent aux environnements applicatifs spécifiques, l'application de vérification de signature doit utiliser un environnement applicatif tenu à jour avec des correctifs de sécurité actualisés.

— OVR-7.7-03: les exigences suivantes spécifiées dans l'ETSI TS 119 101 [1], paragraphe 5.2, s'appliquent à l'application de validation de signature: GSM 1.3.

10) 7.8 Sécurité du réseau

— OVR-7.8-02: si l'accès à distance aux systèmes de stockage ou de traitement de données confidentielles est autorisé, une politique formelle doit être adoptée et décrite dans le cadre des éléments requis par l'OVR-6.3-02.

— OVR-7.8-04: 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.

— OVR-7.8-05: 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.

— OVR-7.8-06: les pare-feu doivent être configurés de manière à empêcher tous les protocoles et accès non nécessaires au fonctionnement du SVSP.

11) 7.12 Plans d'arrêt de fourniture et d'arrêt d'activité du service de validation de signature

— OVR-7.12-02: le plan d'arrêt d'activité du prestataire de services de confiance 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].

12) 7.14 Chaîne d'approvisionnement

— OVR-7.14-01: les exigences spécifiées dans l'ETSI EN 319 401 [2], paragraphe 7.14, s'appliquent.

13) 8.1 Processus de validation des signatures

— VPR-8.1-07: l'application de validation (SVA) doit être conforme aux exigences de l'ETSI TS 119 101 [1], paragraphe 7.4, SIA 1 à SIA 4.

— VPR-8.1-11 [CONDITIONNEL]: si le SVS a pour objet de valider des signatures électroniques qualifiées ou des cachets électroniques qualifiés conformément à l'article 32, paragraphe 1, (ou à l'article 40, selon le cas) du règlement (UE) nº 910/2014 [i.1], le processus de validation doit respecter les exigences de l'ETSI TS 119 172-4 [8].

14) 8.2 Protocole de validation des signatures

— SVP-8.2-03: la réponse de validation de signature doit comporter l'identifiant OID de la politique du SVS.

15) 8.4 Rapport de validation des signatures

— SVR-8.4-02: le rapport de validation doit être conforme à l'ETSI TS 119 102-2 [9].

— SVR-8.4-07 [CONDITIONNEL]: si une politique de validation de signature n'est pas entièrement traitée par le SVS, le rapport doit, outre les contraintes validées, rendre compte des contraintes qui ont été ignorées ou écartées.

— SVR-8.4-15: le rapport de validation doit indiquer clairement l'origine de chaque preuve d'existence (PoE) (au départ de la signature proprement dite, du client, du serveur).

— SVR-8.4-16: le rapport de validation doit être revêtu d'une signature de rapport de validation, qui doit être la signature numérique du SVSP.

— SVR-8.4-17 [CONDITIONNEL]: lorsque les rapports de validation sont signés, le format et la cible de la signature doivent être conformes à l'ETSI TS 119 102-2 [9].

16) 9 Cadre pour la définition des politiques en matière de services de validation fondées sur une politique de services de confiance définie dans le présent document:

— OVR-9-05 [CONDITIONNEL]: lorsqu'une politique de SVS est élaborée sur la base d'une politique de services de confiance définie dans le présent document, une évaluation des risques doit être effectuée afin d'évaluer les exigences opérationnelles et de déterminer les exigences de sécurité à inclure dans la politique applicable à la communauté et à l'applicabilité déclarées.

— OVR-9-06 [CONDITIONNEL]: lorsqu'une politique de SVS est élaborée sur la base d'une politique de services de confiance définie dans le présent document, la politique doit être approuvée et modifiée selon un processus de réexamen défini, comprenant les responsabilités en matière de maintien de la politique.

— OVR-9-07 [CONDITIONNEL]: lorsqu'une politique de SVS est élaborée sur la base d'une politique de services de confiance définie dans le présent document, il doit exister un processus de réexamen défini pour garantir que la politique est prise en charge par les déclarations de pratiques.

— OVR-9-08 [CONDITIONNEL]: lorsqu'une politique de SVS est élaborée sur la base d'une politique de services de confiance définie dans le présent document, le prestataire de services de confiance doit mettre les politiques qu'il prend en charge à la disposition de sa communauté d'utilisateurs.

— OVR-9-09 [CONDITIONNEL]: lorsqu'une politique de SVS est élaborée sur la base d'une politique de services de confiance définie dans le présent document, les révisions apportées aux politiques prises en charge par le prestataire de services de confiance doivent être mises à la disposition des abonnés.

17) Annexe B (normative) – Service de validation qualifié des signatures électroniques qualifiées au sens de l'article 33 du règlement (UE) n° 910/2014:

— VPR-B-02 [CONDITIONNEL]: si le SVSP est un QSVSP, la mise en œuvre doit être conforme à l'ETSI TS 119 172-4 [8].

— REMARQUE 2: vide.

— OVR-B-04 [CONDITIONNEL]: si le SVSP est un QSVSP, les tests prévus dans l'OVR-B-03 doivent vérifier différents cas d'utilisation, positifs et négatifs.

— VPR-B-11 [CONDITIONNEL]: si le SVSP est un QSVSP, le SVSP doit contrôler le calcul de hachage (soit effectuer le calcul du côté serveur, soit contrôler le client s'il y est autorisé du côté client).

— REMARQUE 5: vide.

— REMARQUE 6: vide.

— VPR-B-15 [CONDITIONNEL]: si le SVSP est un QSVSP, afin de satisfaire aux exigences des VPR-B-13 à VPR-B-14, le rapport de validation doit être conforme à l'ETSI TS 119 102-2 [9].

— VPR-B-16 [CONDITIONNEL]: si le SVSP est un QSVSP, la mise en œuvre doit être conforme aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [10] pour l'utilisation de techniques cryptographiques appropriées lors de la fourniture de services de validation qualifiés des signatures électroniques qualifiées.

18) Annexe C (informative) – Mise en correspondance des exigences avec le règlement (UE) nº 910/2014, section «Fourniture d'une validation en conformité avec l'article 32, paragraphe 1», deuxième alinéa:

— Afin de garantir que toutes les conditions requises par l'article 32, paragraphe 1, et l'article 40 du règlement (UE) nº 910/2014 [i.1] sont vérifiées, un algorithme de validation correct est nécessaire. Il fournit le même résultat déterministe pour une signature ou un cachet soumis à validation. La politique de validation de signature est essentielle à cette fin. L'ETSI TS 119 172-4 [8], sur la base de l'algorithme de validation spécifié dans l'ETSI EN 319 102-1 [3], a été publiée dans cette perspective.

2. Pour l'ETSI TS 119 172-4

1) 2.1 Références normatives

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) Signatures électroniques et infrastructures de confiance (ESI) – Procédures de création et de validation des signatures numériques AdES – Partie 1: création et validation.

— Toutes les références à «ETSI TS 119 102-1 [1]» s'entendent comme faites à «ETSI EN 319 102-1 [1]».

— [2] ETSI TS 119 612 V2.3.1 (2024-11) Signatures électroniques et infrastructures (ESI); listes de confiance.

— [13] ETSI TS 119 101 V1.1.1 (2016-03) Signatures électroniques et infrastructures (ESI); Exigences en matière de politique et de sécurité pour les applications de création et de validation de signatures.

2) 4.2 Contraintes et procédures de validation, exigence REQ-4.2-03, section «contraintes de validation X.509», point c):

— i) Si un certificat d'entité finale représente une ancre de confiance, il n'y a pas lieu d'utiliser les contraintes *RevocationCheckingConstraints*.

— ii) Si un certificat d'entité finale ne représente pas une ancre de confiance, la valeur des contraintes *RevocationCheckingConstraints* doit être fixée à «*eitherCheck*» tel que défini dans l'ETSI TS 119 172-1 [3], paragraphe A.4.2.1, tableau A.2, lignes m) 2.1.

— iii) Si un certificat d'entité finale représente une ancre de confiance, il n'y a pas lieu d'utiliser les contraintes *RevocationFreshnessConstraints* définies dans l'ETSI TS 119 172-1 [3], paragraphe A.4.2.1, tableau A.2, lignes m) 2.2.

— iv) Si un certificat d'entité finale ne représente pas une ancre de confiance, les contraintes *RevocationFreshnessConstraints* définies dans l'ETSI TS 119 172-1 [3], paragraphe A.4.2.1, tableau A.2, lignes m) 2.2, doivent être utilisées, la valeur maximale étant de 24 heures pour le certificat de signature. Aucune valeur n'est fixée pour les contraintes *RevocationFreshnessConstraints* dans le cas de certificats autres que le certificat de signature, y compris les certificats à l'appui des horodatages.

3) 4.4 Processus de vérification (des règles) de l'applicabilité technique

— REQ-4.4.2-03: si l'une des vérifications prévues par le REQ-4.4.2-01 échoue, alors:

a) le processus s'arrête;

b) la signature doit être techniquement considérée comme indéterminée, c'est-à-dire comme n'étant ni une signature électronique qualifiée de l'UE, ni un cachet électronique qualifié de l'UE;

c) le résultat ci-dessus et les résultats de processus de tous les processus intermédiaires doivent être pris en compte dans le rapport de vérification relatif aux règles d'applicabilité de la signature.

Journal officiel
de l'Union européenne

FR
Série L

2025/1943

30.9.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/1943 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 certificats qualifiés de signature électronique et aux certificats qualifiés de cachet électronique

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 28, paragraphe 6, et son article 38, paragraphe 6,

considérant ce qui suit:

(1) Les certificats qualifiés de signature électronique et les certificats qualifiés de cachet électronique 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 associant les données de validation de signature électronique ou de validation de cachet électronique à une personne physique ou morale, respectivement, et en confirmant le nom de cette personne, les certificats qualifiés renforcent la certitude quant à l'identité du signataire et du créateur du cachet.

(2) La présomption de conformité prévue à l'article 28, paragraphe 6, et à l'article 38, paragraphe 6, du règlement (UE) nº 910/2014 ne devrait s'appliquer que lorsque les services de confiance qualifiés pour la délivrance de certificats qualifiés de signature électronique et les services de confiance qualifiés pour la délivrance de certificats qualifiés de cachet électronique 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 des services de confiance qualifiés et du contenu des certificats qualifiés.

(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, 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

Normes de référence et spécifications applicables aux certificats qualifiés de signature électronique et de cachet électronique

1. Les normes de référence et les spécifications visées à l'article 28, paragraphe 6, du règlement (UE) n° 910/2014 figurent à l'annexe I du présent règlement.

2. Les normes de référence et les spécifications visées à l'article 38, paragraphe 6, du règlement (UE) n° 910/2014 figurent à l'annexe II 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 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 I

Liste des normes et spécifications de référence pour les certificats qualifiés de signature électronique

Les normes ETSI EN 319 411-2 V2.6.1 («ETSI EN 319 411-2»), ETSI EN 319 412-1 V1.6.1 («ETSI EN 319 412-1»), ETSI EN 319 412-2 V2.4.1 («ETSI EN 319 412-2») et ETSI EN 319 412-5 V2.5.1 («ETSI EN 319 412-5») s'appliquent moyennant les adaptations suivantes:

1. Pour ETSI EN 319 411-2

   1) 2.1 Références normatives

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

   — [2] ETSI EN 319 411-1 V1.5.1 (2025-04) «Signatures électroniques et infrastructures de confiance (ESI) — Exigences de politique et de sécurité applicables aux prestataires de services de confiance délivrant des certificats — Partie 1: Exigences générales», moyennant les adaptations suivantes:

     Clause 2.1 Les références normatives de la norme ETSI EN 319 411-1 V1.5.1 sont modifiées comme suit:

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

     — [10] ETSI EN 319 412-2 V2.4.1 «Signatures électroniques et infrastructures de confiance (ESI) — Profils de certificat — Partie 2: profils des certificats délivrés à des personnes physiques»

     — [14] ETSI EN 319 412-1 V1.6.1 «Signatures électroniques et infrastructures de confiance (ESI) — Profils de certificat — Partie 1: présentation générale et structures de données communes».

   — [3] ETSI EN 319 412-5 V2.5.1 «Signatures électroniques et infrastructures de confiance (ESI) — Profils de certificat — Partie 5: déclarations de certificat qualifié».

   — [5] ETSI EN 319 412-1 V1.6.1 «Signatures électroniques et infrastructures de confiance (ESI) — Profils de certificat — Partie 1: présentation générale et structures de données communes».

   — [6] CEN/TS 419261:2015 «Exigences de sécurité pour systèmes de confiance gérant des certificats et des horodatages».

   — [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]).

   — [8] 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).

   — [9] 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.

   — [10] 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».

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

([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.

2) 5.2 Exigences de l'énoncé des méthodes de certification

— OVR-5.2-02 La ou les CP précisée(s) par la documentation du TSP doivent spécifier les exigences relatives aux profils de certificat à utiliser.

3) 5.3 Nom et identification de la politique de certification

— OVR-5.3-01 Si des modifications ayant une incidence sur l'applicabilité sont apportées à une CP telle que décrite au paragraphe 4.2.2, l'identifiant de la politique doit être modifié.

4) 6.1 Responsabilités de publication et de référentiel

— OVR-6.1-02 Les informations mentionnées au point DIS-6.1-04 de la norme ETSI EN 319 411-1 [2] doivent être mises à la disposition du public au niveau international.

5) 6.2.2 Validation d'identité initiale

— REG-6.2.2-01A La collecte d'attributs et de preuves de l'identité du sujet ainsi que leur validation doivent être précisées conformément aux actes d'exécution adoptés en vertu de l'article 24, paragraphe 1 *quater*, du règlement (UE) nº 910/2014 [i.1].

— REG-6.2.2-02 [QCP-n] et [QCP-n-qscd] L'identité de la personne physique et, le cas échéant, tout attribut spécifique de cette personne, doivent être vérifiés conformément aux actes d'exécution adoptés en vertu de l'article 24, paragraphe 1 *quater*, du règlement (UE) nº 910/2014 [i.1].

— NOTE 1: vide.

6) 6.3.3 Délivrance du certificat

— GEN-6.3.3-01 Les exigences GEN-6.3.3-01 à GEN-6.3.3-10 identifiées dans l'ETSI EN 319 411-1 [2], paragraphe 6.3.3, doivent s'appliquer.

— GEN-6.3.3-02 [CONDITIONNEL] Si un certificat est délivré à une personne physique identifiée en association avec la personne morale, les attributs du sujet identifiant l'organisation dans le certificat représentent la personne morale ou la sous-entité de cette personne morale et l'identifiant du sujet dans le certificat est la personne physique.

— GEN-6.3.3-03 L'identifiant de la CP est [CHOIX]:

a) [QCP-n]

— comme spécifié au paragraphe 5.3, point a), et/ou

— un OID, attribué par le TSP, une autre partie prenante concernée ou une normalisation supplémentaire pour une politique de certification améliorant les exigences de politique applicables correspondantes définies dans le présent document.

b) [QCP-n-qscd]

— comme spécifié au paragraphe 5.3, point c), et/ou

— un OID, attribué par le TSP, une autre partie prenante concernée ou un autre organisme de normalisation pour une politique de certificat renforçant les exigences de politique applicables correspondantes définies dans le présent document.

7) 6.3.5 Utilisation de la paire de clés et du certificat

— SDP-6.3.5-02A [CONDITIONNEL] Si le TSP gère le QSCD pour le sujet, le TSP doit être un prestataire de services de confiance qualifié fournissant un service de confiance qualifié pour la gestion d'un dispositif de création de signature électronique qualifié à distance, conformément au règlement (UE) nº 910/2014 [i.1].

— SDP-6.3.5-11A Les obligations de l'abonné (voir paragraphe 6.3.4) doivent comprendre, si l'abonné ou le sujet génère les clés du sujet:

a) une obligation de générer les clés du sujet à l'aide d'un algorithme conforme aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité [7] et publiés par l'ENISA pour les utilisations de la clé certifiée telles qu'identifiées dans la CP;

b) une obligation d'utiliser une longueur de clé et un algorithme conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité [7] et publiés par l'ENISA pour les utilisations de la clé certifiée telles qu'identifiées dans la CP pendant la durée de validité du certificat.

8) 6.3.10 Services de statut de certificat

— CSS-6.3.10-08 [CONDITIONNEL] Si des CRL sont fournies, il convient que le TSP préserve l'intégrité et la disponibilité de la dernière CRL au moins pendant la période spécifiée dans le CPS, comme exigé dans CSS-6.3.10-12.

9) 6.4.4 Contrôles du personnel

— OVR-6.4.4-02 Le personnel employé par le TSP dans des rôles de confiance et, le cas échéant, les sous-traitants du TSP intervenant dans des rôles de confiance, doivent pouvoir satisfaire à l'exigence relative aux connaissances spécialisées, à l'expérience et aux qualifications 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 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.

— OVR-6.4.4-04 Outre les rôles de confiance définis dans ETSI EN 319 401 [1] (paragraphe 7.2-15), les rôles de confiance des agents chargés de l'enregistrement et de la révocation ayant des responsabilités telles que définies dans la norme TS 419261 [6] doivent être pris en charge. Lorsque le QTSP est directement géré par un État membre ou un organisme du secteur public ou est géré pour le compte d'un État membre ou d'un organisme du secteur public, ces rôles de confiance supplémentaires peuvent être assumés par un ou plusieurs représentants officiels agissant au nom et pour le compte des agents chargés de l'enregistrement et de la révocation travaillant dans les administrations locales ou régionales.

10) 6.4.9 Cessation d'activité de la CA ou de la RA

— OVR-6.4.9-02 Le plan de cessation d'activité du TSP doit satisfaire 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].

11) 6.5.1 Génération et installation d'une paire de clés

— OVR-6.5.1-01A La paire de clés de la CA doit être générée à l'aide d'un algorithme conforme aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [7] aux fins de la signature de la CA.

— OVR-6.5.1-01B La longueur de clé et l'algorithme sélectionnés pour la clé de signature de la CA doivent être conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [7] aux fins de la signature de la CA.

— OVR-6.5.1-01C [CONDITIONNEL] Si la CA génère les clés du sujet, celles-ci doivent être conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [7] aux fins indiquées dans la CP pendant la durée de validité du certificat.

12) 6.5.2 Contrôles techniques de protection de la clé privée et du module cryptographique

— GEN-6.5.2-01 Toutes les exigences identifiées dans l'ETSI EN 319 411-1 [2], paragraphe 6.5.2, doivent s'appliquer, à l'exception des exigences OVR-6.5.2-01, OVR-6.5.2-03 et OVR-6.5.2-04.

— GEN-6.5.2-02 Les paires de clés du TSP, y compris les clés utilisées par les services de révocation et d'enregistrement, doivent être générées dans un dispositif cryptographique sécurisé qui est un système fiable certifié conformément:

— 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 [10] 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

— au schéma européen commun de certification de cybersécurité fondé sur des critères communs (EUCC) [8] [9] et certifié au niveau EAL 4 ou supérieur; ou

— jusqu'au 31.12.2030, à la norme FIPS PUB 140-3 [11] 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 [8] [9], ce dispositif doit être configuré et utilisé conformément à cette certification.

— GEN-6.5.2-03 La clé de signature privée de la CA doit être stockée et utilisée dans un appareil cryptographique sécurisé répondant aux exigences des points GEN-6.5.2-01 et GEN-6.5.2-02.

13) 6.5.7 Contrôles de sécurité du réseau

— OVR-6.5.7-02 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-6.5.7-03 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-6.5.7-04 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.

14) 6.6.1 Profil de certificat

— GEN-6.6.1-05 Le certificat comprend l'un des identifiants de politique identifiés dans GEN-6.3.3-03 [CHOIX]. Le certificat peut inclure d'autres OID attribués par le TSP.

2. Pour ETSI EN 319 412-2

1) 2.1 Références normatives

— [2] ETSI EN 319 412-5 V2.5.1 «Signatures électroniques et infrastructures de confiance (ESI) — Profils de certificat — Partie 5: déclarations de certificat qualifié».

— [9] Groupe européen de certification de cybersécurité, sous-groupe sur la cryptographie «Mécanismes cryptographiques agréés», publié par l'ENISA.

2) 4.2.2 Signature

— GEN-4.2.2-2 Il convient de sélectionner l'algorithme de signature conformément aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [9].

— NOTE vide.

3) 4.2.3.1 Personnes morales émettrices

— GEN-4.2.3.1-3 S'il est connu qu'un numéro d'immatriculation approprié existe, l'identité de l'émetteur doit contenir l'attribut *organizationIdentifier*, la valeur de ce numéro d'immatriculation correspondant à celle indiquée dans le registre officiel établissant ce numéro d'immatriculation.

4) 4.2.5 Informations de clé publique du sujet

— GEN-4.2.5-2 Il convient de sélectionner la clé publique du sujet conformément aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [9].

— NOTE vide.

5) 4.2.6 Numéro de série

— GEN-4.2.6-01 Chaque certificat délivré par le TSP doit avoir un numéro de série *serialNumber* (tel que spécifié dans la clause 4.1.2.2 de la RFC 5280 [1] de l'IETF) unique.

ANNEXE II

Liste des normes et spécifications de référence pour les certificats qualifiés de signature électronique

Les normes ETSI EN 319 411-2 V2.6.1 («ETSI EN 319 411-2»), ETSI EN 319 412-1 V1.6.1 («ETSI EN 319 412-1»), ETSI EN 319 412-3 V1.3.1 («ETSI EN 319 412-3»), ETSI EN 319 412-2 V2.4.1 («ETSI EN 319 412-2») et ETSI EN 319 412-5 V2.5.1 («ETSI EN 319 412-5») s'appliquent moyennant les adaptations suivantes:

1. Pour ETSI EN 319 411-2

1) 2.1 Références normatives

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

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) «Signatures électroniques et infrastructures de confiance (ESI) — Exigences de politique et de sécurité applicables aux prestataires de services de confiance délivrant des certificats — Partie 1: Exigences générales», moyennant les adaptations suivantes:

Clause 2.1 Les références normatives de la norme ETSI EN 319 411-1 V1.5.1 sont modifiées comme suit:

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

— [10] ETSI EN 319 412-2 V2.4.1 «Signatures électroniques et infrastructures de confiance (ESI) — Profils de certificat — Partie 2: profils des certificats délivrés à des personnes physiques».

— [14] ETSI EN 319 412-1 V1.6.1 «Signatures électroniques et infrastructures de confiance (ESI) — Profils de certificat — Partie 1: présentation générale et structures de données communes».

— [3] ETSI EN 319 412-5 V2.5.1 «Signatures électroniques et infrastructures de confiance (ESI) — Profils de certificat — Partie 5: déclarations de certificat qualifié».

— [5] ETSI EN 319 412-1 V1.6.1 «Signatures électroniques et infrastructures de confiance (ESI) — Profils de certificat — Partie 1: présentation générale et structures de données communes».

— [6] CEN/TS 419261: 2015 «Exigences de sécurité pour systèmes de confiance gérant des certificats et des horodatages», (élaborées par le CEN).

— [7] Groupe européen de certification de cybersécurité, sous-groupe sur la cryptographie: «Agreed Cryptographic Mechanisms» publié par l'ENISA.

— [8] Règlement d'exécution (UE) 2024/482 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).

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

— [10] ISO/IEC 15408: 2022 (parties 1 à 5) «Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation de la sécurité informatique».

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

2) 5.2 Exigences de l'énoncé des méthodes de certification

— OVR-5.2-02 La ou les CP précisée(s) par la documentation du TSP doit spécifier les exigences relatives aux profils de certificat à utiliser.

3) 5.3 Nom et identification de la politique de certification

— OVR-5.3-01 Si des modifications ayant une incidence sur l'applicabilité sont apportées à une CP telle que décrite au paragraphe 4.2.2, l'identifiant de la politique doit être modifié.

4) 6.1 Responsabilités de publication et de référentiel

— OVR-6.1-02 Les informations mentionnées au point DIS-6.1-04 de l'ETSI EN 319 411-1 [2] doivent être mises à la disposition du public au niveau international.

5) 6.2.2 Validation d'identité initiale

— REG-6.2.2-01A La collecte d'attributs et de preuves de l'identité du sujet ainsi que leur validation doivent être précisées conformément aux actes d'exécution adoptés en vertu de l'article 24, paragraphe 1 *quater*, du règlement (UE) nº 910/2014 [i.1].

— REG-6.2.2-03 [QCP-l] et [QCP-l-qscd] L'identité de la personne physique et, le cas échéant, tout attribut spécifique de la personne, doivent être vérifiés conformément aux actes d'exécution adoptés en vertu de l'article 24, paragraphe 1 *quater*, du règlement (UE) nº 910/2014 [i.1].

— NOTE 3 Voir note 2.

6) 6.3.3 Délivrance du certificat

— GEN-6.3.3-01 Les exigences GEN-6.3.3-01 à GEN-6.3.3-10 identifiées dans l'ETSI EN 319 411-1 [2], paragraphe 6.3.3, doivent s'appliquer.

— GEN-6.3.3-02 L'identifiant de la CP doit être [CHOIX]:

a) [QCP-l]

— comme spécifié au paragraphe 5.3, point b), et/ou

— un OID, attribué par le TSP, une autre partie prenante concernée ou une normalisation supplémentaire pour une politique de certification améliorant les exigences de politique applicables correspondantes définies dans le présent document.

b) [QCP-l-qscd]

— comme spécifié au paragraphe 5.3, point d), et/ou

— un OID, attribué par le TSP, une autre partie prenante concernée ou une normalisation supplémentaire pour une politique de certification améliorant les exigences de politique applicables correspondantes définies dans le présent document.

7) 6.3.5 Utilisation de la paire de clés et du certificat

— SDP-6.3.5-02A [CONDITIONNEL] Si le TSP gère le QSCD pour le sujet, le TSP doit être un prestataire de services de confiance qualifié fournissant un service de confiance qualifié pour la gestion d'un dispositif de création de cachet électronique qualifié à distance, conformément au règlement (UE) nº 910/2014 [i.1].

— SDP-6.3.5-11A Les obligations de l'abonné (voir paragraphe 6.3.4) comprennent, si l'abonné ou le sujet génère les clés du sujet:

a) une obligation de générer les clés du sujet à l'aide d'un algorithme conforme aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [7] pour les utilisations de la clé certifiée telles qu'identifiées dans la CP; et

b) une obligation d'utiliser une longueur de clé et un algorithme conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [7] pour les utilisations de la clé certifiée telles qu'identifiées dans la CP durant la période de validité du certificat.

8) 6.3.10 Services de statut de certificat

— CSS-6.3.10-08 [CONDITIONNEL] Si des CRL sont fournies, il convient que le TSP préserve l'intégrité et la disponibilité de la dernière CRL au moins pendant la période spécifiée dans le CPS, comme exigé dans CSS-6.3.10-12.

9) 6.4.4 Contrôles du personnel

— OVR-6.4.4-02 Le personnel employé par le TSP dans des rôles de confiance et, le cas échéant, les sous-traitants du TSP intervenant dans des rôles de confiance, doivent pouvoir satisfaire à l'exigence relative aux connaissances spécialisées, à l'expérience et aux qualifications 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 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.

— OVR-6.4.4-04 Outre les rôles de confiance définis dans ETSI EN 319 401 [1] (paragraphe 7.2-15), les rôles de confiance des agents chargés de l'enregistrement et de la révocation ayant des responsabilités telles que définies dans la norme TS 419261 [6] doivent être pris en charge. Lorsque le QTSP est directement géré par un État membre ou un organisme du secteur public ou est géré pour le compte d'un État membre ou d'un organisme du secteur public, ces rôles de confiance supplémentaires peuvent être assumés par un ou plusieurs représentants officiels agissant au nom et pour le compte des agents chargés de l'enregistrement et de la révocation travaillant dans les administrations locales ou régionales.

10) 6.4.9 Cessation d'activité de la CA ou de la RA

— OVR-6.4.9-02 Le plan de cessation d'activité du TSP doit satisfaire 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].

11) 6.5.1 Génération et installation d'une paire de clés

— OVR-6.5.1-01A La paire de clés de la CA doit être générée à l'aide d'un algorithme conforme aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [7] aux fins de la signature de la CA.

— OVR-6.5.1-01B La longueur de clé et l'algorithme sélectionnés pour la clé de signature de la CA doivent être conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [7] aux fins de la signature de la CA.

— OVR-6.5.1-01C [CONDITIONNEL] Si la CA génère les clés du sujet, celles-ci doivent être conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [7] aux fins indiquées dans la CP pendant la durée de validité du certificat.

12) 6.5.2 Contrôles techniques de protection de la clé privée et du module cryptographique

— GEN-6.5.2-01 Toutes les exigences identifiées dans l'ETSI EN 319 411-1 [2], paragraphe 6.5.2, doivent s'appliquer, à l'exception des exigences OVR-6.5.2-01, OVR-6.5.2-03 et OVR-6.5.2-04.

— GEN-6.5.2-02 Les paires de clés du TSP, y compris les clés utilisées par les services de révocation et d'enregistrement, doivent être générées dans un dispositif cryptographique sécurisé qui est un système fiable certifié conformément:

  — 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 [10] 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

  — au schéma européen commun de certification de cybersécurité fondé sur des critères communs (EUCC) [8] [9] et certifié au niveau EAL 4 ou supérieur; ou

  — jusqu'au 31.12.2030, à la norme FIPS PUB 140-3 [11] 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 [8] [9], ce dispositif doit être configuré et utilisé conformément à cette certification.

— GEN-6.5.2-03 La clé de signature privée de la CA doit être stockée et utilisée dans un appareil cryptographique sécurisé répondant aux exigences des points GEN-6.5.2-01 et GEN-6.5.2-02.

13) 6.5.7 Contrôles de sécurité du réseau

— OVR-6.5.7-02 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.

— OVR-6.5.7-03 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.

— OVR-6.5.7-04 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.

14) 6.6.1 Profil de certificat

— GEN-6.6.1-05 Le certificat doit inclure l'un des identificateurs de politique définis dans GEN-6.3.3-02 [CHOIX].

2. Pour ETSI EN 319 412-3

1) 2.1 Références normatives

— [2] ETSI EN 319 412-2 V2.4.1 «Signatures électroniques et infrastructures de confiance (ESI) — Profils de certificat — Partie 2: profils des certificats délivrés à des personnes physiques».

2) 4.2.1 Sujet

— LEG-4.2.1-6 L'attribut *organizationIdentifier* doit contenir une identification de l'organisation du sujet qui est différente du nom de l'organisation. S'il est connu qu'un numéro d'immatriculation approprié existe, l'attribut *organizationIdentifier* doit contenir une valeur de ce numéro d'immatriculation correspondant à celle indiquée dans le registre officiel établissant ce numéro d'immatriculation.

3. Pour ETSI EN 319 412-2

1) 2.1 Références normatives

— [2] ETSI EN 319 412-5 V2.5.1 «Signatures électroniques et infrastructures de confiance (ESI) — Profils de certificat — Partie 5: déclarations de certificat qualifié».

— [9] Groupe européen de certification de cybersécurité, sous-groupe sur la cryptographie: «Agreed Cryptographic Mechanisms» publié par l'ENISA.

2) 2.2 Références informatives

— [i.7] vide.

3) 4.2.2 Signature

— GEN-4.2.2-2 Il convient de sélectionner l'algorithme de signature conformément aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [9].

— NOTE vide.

4) 4.2.3.1 Personnes morales émettrices

— GEN-4.2.3.1-3 S'il est connu qu'un numéro d'immatriculation approprié existe, l'identité de l'émetteur doit contenir l'attribut *organizationIdentifier*, la valeur de ce numéro d'immatriculation correspondant à celle indiquée dans le registre officiel établissant ce numéro d'immatriculation.

5) 4.2.5 Informations de clé publique du sujet

— GEN-4.2.5-2 Il convient de sélectionner la clé publique du sujet conformément aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [9].

— NOTE vide.

6) 4.2.6 Numéro de série

— GEN-4.2.6-01 Chaque certificat délivré par le TSP doit avoir un numéro de série *serialNumber* (tel que spécifié dans la clause 4.1.2.2 de la RFC 5280 [1] de l'IETF) unique.

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.

Journal officiel
de l'Union européenne

FR
Série L

2025/1945

30.9.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/1945 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 la validation des signatures électroniques qualifiées et des cachets électroniques qualifiés et la validation des signatures électroniques avancées reposant sur des certificats qualifiés et des cachets électroniques avancés reposant sur des certificats 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 32, paragraphe 3, son article 32 *bis*, paragraphe 3, son article 40 et son article 40 *bis*,

considérant ce qui suit:

(1) Les signatures électroniques qualifiées, les cachets électroniques qualifiés, les signatures électroniques avancées reposant sur des certificats qualifiés de signature électronique et les cachets électroniques avancés reposant sur des certificats qualifiés de cachet électronique, à condition que leur validité puisse être confirmée, garantissent aux parties utilisatrices l'intégrité et l'authenticité des données munies de la signature ou du cachet et renforcent la certitude quant à l'identité du signataire ou du créateur de cachet. Ces signatures électroniques et ces cachets électroniques 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.

(2) La présomption de conformité prévue à l'article 32, paragraphe 1, à l'article 40, à l'article 32 *bis*, paragraphe 3, et à l'article 40 *bis* du règlement (UE) nº 910/2014 devrait s'appliquer lorsque les processus de validation des signatures électroniques qualifiées, des cachets électroniques qualifiés, des signatures électroniques avancées reposant sur des certificats qualifiés de signature électronique et des cachets électroniques avancés reposant sur des certificats qualifiés de cachet électronique sont conformes aux normes techniques 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 capacité de vérifier la validité technique de ces signatures et cachets et, le cas échéant, leur statut qualifié.

(3) 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.

(4) 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).

(5) 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.

(6) Les mesures prévues par le présent règlement sont conformes à l'avis du comité institué par l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Normes et spécifications de référence

1. Les normes de référence et les spécifications visées à l'article 32, paragraphe 3, et à l'article 40 du règlement (UE) nº 910/2014 figurent à l'annexe I du présent règlement.

2. Les normes de référence et les spécifications visées à l'article 32 *bis*, paragraphe 3, et à l'article 40 *bis* du règlement (UE) nº 910/2014 figurent à l'annexe II 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 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) nº 45/2001 et la décision nº 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 et spécifications de référence pour la validation des signatures électroniques qualifiées et des cachets électroniques qualifiés

Les normes ETSI TS 119 172-4 V1.1.1 (2021-05) ([1]) («ETSI TS 119 172-4») et ETSI TS 119 102-2 V1.4.1 (2023-06) ([2]) («ETSI TS 119 102-2») s'appliquent moyennant les adaptations suivantes:

1. Pour l'ETSI TS 119 172-4

   1) 2.1 Références normatives:

      — [1] ETSI EN 319 102-1 V1.4.1 (2024-06) Signatures électroniques et infrastructures de confiance (ESI) — Procédures de création et de validation des signatures numériques AdES — Partie 1: création et validation.

      — Toutes les références à «ETSI TS 119 102-1 [1]» s'entendent comme faites à «ETSI EN 319 102-1 [1]».

      — [2] ETSI TS 119 612 V2.3.1 (2024-11) Signatures électroniques et infrastructures (ESI); Listes de confiance.

      — [13] ETSI TS 119 101 V1.1.1 (2016-03) Signatures électroniques et infrastructures (ESI) - Exigences en matière de politique et de sécurité pour les applications de création et de validation de signatures.

   2) 4.2 Contraintes et procédures de validation, exigence REQ-4.2-03, section «contraintes de validation X.509», point c):

      — i) Si un certificat d'entité finale représente une ancre de confiance, il n'y a pas lieu d'utiliser les contraintes RevocationCheckingConstraints.

      — ii) Si un certificat d'entité finale ne représente pas une ancre de confiance, la valeur des contraintes RevocationCheckingConstraints doit être fixée à «eitherCheck» tel que défini dans l'ETSI TS 119 172-1 [3], paragraphe A.4.2.1, tableau A.2, lignes m) 2.1.

      — iii) Si un certificat d'entité finale représente une ancre de confiance, il n'y a pas lieu d'utiliser les contraintes RevocationFreshnessConstraints définies dans l'ETSI TS 119 172-1 [3], paragraphe A.4.2.1, tableau A.2, lignes m) 2.2.

      — iv) Si un certificat d'entité finale ne représente pas une ancre de confiance, les contraintes Revocation-FreshnessConstraints définies dans l'ETSI TS 119 172-1 [3], paragraphe A.4.2.1, tableau A.2, lignes m) 2.2, doivent être utilisées, la valeur maximale étant de 24 heures pour le certificat de signature. Aucune valeur n'est fixée pour les contraintes *RevocationFreshnessConstraints* pour les certificats autres que le certificat de signature, y compris les certificats à l'appui des horodatages.

   3) 4.3 Exigences relatives aux pratiques en matière de validation des signatures et de vérification des règles d'applicabilité

      — REQ-4.3-02: les applications de validation de signature doivent être conformes à l'ETSI TS 119 101 [13].

([1]) ETSI TS 119 172-4 — Signatures électroniques et infrastructures (ESI) — Politiques de signature — Partie 4: (politique de validation des) règles d'applicabilité des signatures pour les signatures électroniques qualifiées et les cachets électroniques qualifiés européens utilisant des listes de confiance, V1.1.1 (2021-05).

([2]) ETSI TS 119 102-2 — Signatures électroniques et infrastructures (ESI) — Procédures de création et de validation des signatures numériques AdES — Partie 2: rapport de validation de signature, V1.4.1 (2023-06).

4) 4.4 Processus de vérification (des règles) de l'applicabilité technique

— REQ-4.4.2-03: si l'une des vérifications prévues par le REQ-4.4.2-01 échoue, alors:

a) le processus s'arrête;

b) la signature doit être techniquement considérée comme indéterminée, c'est-à-dire comme n'étant ni une signature électronique qualifiée de l'UE, ni un cachet électronique qualifié de l'UE; et

c) le résultat ci-dessus et les résultats de tous les processus intermédiaires doivent être pris en compte dans le rapport de vérification relatif aux règles d'applicabilité de la signature.

ANNEXE II

Liste des normes et spécifications de référence pour la validation des signatures électroniques avancées reposant sur des certificats qualifiés et des cachets électroniques avancés reposant sur des certificats qualifiés

Les normes ETSI TS 119 172-4 V1.1.1 (2021-05) ([1]) («ETSI TS 119 172-4») et ETSI TS 119 102-2 V1.4.1 (2023-06) ([2]) («ETSI TS 119 102-2») s'appliquent moyennant les adaptations suivantes:

1. Pour l'ETSI TS 119 172-4

   1) 2.1 Références normatives:

      — [1] ETSI EN 319 102-1 V1.4.1 (2024-06) Signatures électroniques et infrastructures de confiance (ESI) — Procédures de création et de validation des signatures numériques AdES — Partie 1: création et validation.

      — Toutes les références à «ETSI TS 119 102-1 [1]» s'entendent comme faites à «ETSI EN 319 102-1 [1]».

      — [2] ETSI TS 119 612 V2.3.1 (2024-11) Signatures électroniques et infrastructures (ESI) - Listes de confiance.

      — [13] ETSI TS 119 101 V1.1.1 (2016-03) Signatures électroniques et infrastructures (ESI) — Exigences en matière de politique et de sécurité pour les applications de création et de validation de signatures.

   2) 4.2 Contraintes et procédures de validation, exigence REQ-4.2-03, section «contraintes de validation X.509», point c):

      — i) Si un certificat d'entité finale représente une ancre de confiance, il n'y a pas lieu d'utiliser les contraintes *RevocationCheckingConstraints*.

      — ii) Si un certificat d'entité finale ne représente pas une ancre de confiance, la valeur des contraintes *RevocationCheckingConstraints* doit être fixée à «*eitherCheck*» tel que défini dans l'ETSI TS 119 172-1 [3], paragraphe A.4.2.1, tableau A.2, lignes m) 2.1.

      — iii) Si un certificat d'entité finale représente une ancre de confiance, il n'y a pas lieu d'utiliser les contraintes *RevocationFreshnessConstraints* définies dans l'ETSI TS 119 172-1 [3], paragraphe A.4.2.1, tableau A.2, lignes m) 2.2.

      — iv) Si un certificat d'entité finale ne représente pas une ancre de confiance, les contraintes *RevocationFreshnessConstraints* définies dans l'ETSI TS 119 172-1 [3], paragraphe A.4.2.1, tableau A.2, lignes m) 2.2, doivent être utilisées, la valeur maximale étant de 24 heures pour le certificat de signature. Aucune valeur n'est fixée pour les contraintes *RevocationFreshnessConstraints* pour les certificats autres que le certificat de signature, y compris les certificats à l'appui des horodatages.

   3) 4.3 Exigences relatives aux pratiques en matière de validation des signatures et de vérification des règles d'applicabilité

      — REQ-4.3-02: les applications de validation de signature doivent être conformes à l'ETSI TS 119 101 [13].

   4) 4.4 Processus de vérification (des règles) de l'applicabilité technique

      — REQ-4.4.2-03: si l'une des vérifications prévues par le REQ-4.4.2-01 échoue, alors:

         a) le processus s'arrête;

         b) la signature doit être techniquement déterminée comme étant indéterminée, c'est-à-dire comme n'étant ni une signature électronique avancée fondée sur un certificat qualifié de l'UE, ni un cachet électronique avancé fondé sur un certificat qualifié de l'UE; et

([1]) ETSI TS 119 172-4 — Signatures électroniques et infrastructures (ESI) — Politiques de signature — Partie 4: (politique de validation des) règles d'applicabilité des signatures pour les signatures électroniques qualifiées et les cachets électroniques qualifiés européens utilisant des listes de confiance, V1.1.1 (2021-05).

([2]) ETSI TS 119 102-2 — Signatures électroniques et infrastructures (ESI) — Procédures de création et de validation des signatures numériques AdES — Partie 2: rapport de validation de signature, V1.4.1 (2023-06).

c) le résultat ci-dessus et les résultats des processus de tous les processus intermédiaires doivent être pris en compte dans le rapport de vérification relatif aux règles d'applicabilité de la signature.

— REQ-4.4.2-04: vide.

— REQ-4.4.2-05: vide.

— REQ-4.4.2-06: à ce stade du processus de vérification (des règles) de l'applicabilité technique (TARC), si les conditions suivantes sont remplies:

a) le certificat de signature est déterminé, au «best signature time», comme étant un certificat qualifié de signature électronique (ou de cachet électronique, selon le cas) de l'UE, comme spécifié dans le REQ-4.4.2-02, point a); et

b) le résultat du processus exécuté conformément au paragraphe 4.2 du présent document est TOTAL-PASSED,

alors la signature numérique doit être déterminée comme étant techniquement appropriée pour mettre en œuvre une signature électronique avancée de l'UE fondée sur un certificat qualifié (ou un cachet électronique avancé de l'UE fondé sur un certificat qualifié, selon le cas), sinon la signature n'est pas déterminée techniquement ni comme une signature électronique avancée de l'UE fondée sur un certificat qualifié, ni comme un cachet électronique avancé de l'UE fondé sur un certificat qualifié.

Journal officiel
de l'Union européenne

FR
Série L

2025/1946

30.9.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/1946 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 services qualifiés de préservation des signatures électroniques qualifiées et des cachets 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 34, paragraphe 2, et son article 40,

considérant ce qui suit:

(1) Les services qualifiés de préservation des signatures électroniques qualifiées et des cachets électroniques qualifiés garantissent, sur le long terme, l'intégrité, l'authenticité, la preuve de l'existence et l'accessibilité des preuves de préservation de ces signatures électroniques et cachets électroniques. Cela permet de démontrer leur validité juridique sur des périodes prolongées et garantit la possibilité de les valider, quelles que soient les évolutions technologiques futures. Ces services sont fournis de manière indépendante ou dans le cadre d'un autre service de confiance qualifié, tel que des services d'archivage électronique qualifiés.

(2) La présomption de conformité prévue à l'article 34, paragraphe 1 *bis*, et à l'article 40 du règlement (UE) nº 910/2014 ne devrait s'appliquer que lorsque les services qualifiés de préservation des signatures électroniques qualifiées et des cachets électroniques 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 la capacité de vérifier le statut qualifié et la validité technique des signatures et des cachets au fil du temps.

(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, 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).

(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.

(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) nº 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Normes et spécifications de référence

Les normes de référence et les spécifications visées à l'article 34, paragraphe 2, et à l'article 40 du règlement (UE) nº 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 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) nº 45/2001 et la décision nº 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 de référence et des spécifications mentionnées à l'article 2

Les normes ETSI TS 119 511 V1.1.1 (2019-06) («ETSI TS 119 511») et ETSI TS 119 172-4 V1.1.1 (2021-05) («ETSI TS 119 172-4») s'appliquent moyennant les adaptations suivantes:

1. Pour ETSI TS 119 511

1) 2.1 Références normatives:

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

— [2] ETSI TS 119 612 (V2.3.1) «Electronic Signatures and Infrastructures (ESI); Trusted Lists».

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

— [6] Règlement d'exécution (UE) 2024/482 de la Commission ([1]) 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).

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

— [8] 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]).

— [9] ETSI TS 119 172-4 V1.1.1 (2021-05) «Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists».

— [10] 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) 3.1 Termes

— 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.

3) 6.4 Profils de préservation

— OVR-6.4-08A [WTS] [WOS] La durée attendue des preuves doit être conforme aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [8].

— NOTE 3 vide.

4) 6.5 Politique de préservation des éléments de preuve

— OVR-6.5-04A Les algorithmes cryptographiques utilisés doivent être conformes aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [8].

— NOTE 1 vide.

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

5) 7.2 Ressources humaines

— OVR-7.2-02 Le personnel employé par le PSP (fournisseur du service de préservation) dans des rôles de confiance et, le cas échéant, les sous-traitants du PSP intervenant dans des rôles de confiance, doivent être en mesure de satisfaire à l'exigence concernant les «connaissances spécialisées, l'expérience et les qualifications» grâce à une formation formelle et à des certificats, ou de manière empirique, ou par une combinaison des deux.

— OVR-7.2-03 La conformité au point OVR-7.2-02 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.

6) 7.5 Contrôles cryptographiques

— OVR-7.5-05 [CONDITIONNEL] Lorsque le PSP signe (une partie d') une preuve de préservation, la clé de signature privée du PSP doit être stockée 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 [10] 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 [6] [7] et certifié au niveau EAL 4 ou supérieur; ou

c) jusqu'au 31.12.2030, à la norme FIPS PUB 140-3 [5] 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 [6] [7], ce dispositif doit être configuré et utilisé conformément à cette certification.

— OVR-7.5-06 [CONDITIONNEL] vide.

— OVR-7.5-07 [CONDITIONNEL] Lorsque le PSP signe (une partie d') une preuve de préservation, les éventuelles copies de sauvegarde des clés de signature privée du PSP doivent être protégées afin que leur intégrité et leur confidentialité soient garanties par le dispositif cryptographique sécurisé, avant qu'elles soient stockées à l'extérieur de ce dispositif.

— OVR-7.5-08 Toute exportation ou importation de clé de signature privée d'un PSP 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) 7.8 Sécurité du réseau

— OVR-7.8-03 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-7.8-04 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-7.8-05 Les pare-feu doivent être configurés de manière à empêcher tous les protocoles et accès non nécessaires au fonctionnement du PSP.

8) 7.14 Surveillance cryptographique

— OVR-7.14-03A L'évaluation des algorithmes cryptographiques dans OVR-7.14.01 et OVR-7.14.02 est conforme aux mécanismes cryptographiques agréés approuvés par le groupe européen de certification de cybersécurité et publiés par l'ENISA [8].

— NOTE vide.

9) 7.12 Cessation d'activité et plans de cessation du TSP

— OVR-7.12-01A Le plan de cessation d'activité 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.2].

10) 7.17 Chaîne d'approvisionnement

— OVR-7.17-01 Les exigences spécifiées dans l'ETSI EN 319 401 [1], paragraphe 7.14, doivent s'appliquer.

11) Annexe A (normative): Service qualifié de préservation pour QES au sens de l'article 34 du règlement (UE) nº 910/2014

— OVR-A-02 [PDS] [PDS + PGD]

a) le service de préservation doit conserver toutes les informations nécessaires pour vérifier le statut qualifié de la signature ou du cachet électronique, qui ne seraient pas accessibles au public avant la fin de la période de préservation;

b) le service de préservation doit veiller à ce que, à tout moment au cours de la période de préservation, les informations préservées soient telles que, lorsqu'elles sont fournies pour alimenter le processus spécifié dans l'ETSI TS 119 172-4 [9], paragraphe 4.4, le résultat de ce processus détermine clairement si la signature ou le cachet numérique étaient, au moment de leur préservation, techniquement appropriés pour la mise en œuvre d'une signature électronique qualifiée de l'UE ou d'un cachet électronique qualifié de l'UE.

— OVR-A-03 [PDS] [PDS + PGD] Il convient que les horodatages utilisés dans les preuves de préservation soient des horodatages qualifiés conformément au règlement (UE) nº 910/2014 [i.2].

2. Pour ETSI TS 119 172-4

1) 2.1 Références normatives:

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) «Signatures électroniques et infrastructures (ESI) — Modes opératoires pour la création et la validation des signatures numériques AdES; Partie 1: création et validation».

— Toutes les références à «ETSI TS 119 102-1 [1]» s'entendent comme faites à «ETSI EN 319 102-1 [1]».

— [2] ETSI TS 119 612 (V2.3.1) «Electronic Signatures and Infrastructures (ESI); Trusted Lists».

— [13] ETSI TS 119 101 V1.1.1 (2016-03) «Electronic Signatures and Infrastructures (ESI) — Policy and security requirements for applications for signature creation and signature validation».

2) 4.2 Contraintes et procédures de validation, exigence REQ-4.2-03, section «contraintes de validation X.509», point c):

— (i) Si un certificat d'entité finale représente une ancre de confiance, il n'y a pas lieu d'utiliser les contraintes *RevocationCheckingConstraints*.

— (ii) Si un certificat d'entité finale ne représente pas une ancre de confiance, la valeur des contraintes *RevocationCheckingConstraints* doit être fixée à «*eitherCheck*» tel que défini dans l'ETSI TS 119 172-1 [3], paragraphe A.4.2.1, tableau A.2, lignes m) 2.1.

— (iii) Si un certificat d'entité finale représente une ancre de confiance, il n'y a pas lieu d'utiliser les contraintes *RevocationFreshnessConstraints* définies dans l'ETSI TS 119 172-1 [3], paragraphe A.4.2.1, tableau A.2, lignes m) 2.2.

— (iv) Si un certificat d'entité finale ne représente pas une ancre de confiance, les contraintes «*RevocationFreshnessConstraints*» définies dans l'ETSI TS 119 172-1 [3], paragraphe A.4.2.1, tableau A.2, lignes m) 2.2, doivent être utilisées, la valeur maximale étant de 0 pour le certificat de signature, en veillant à ce que les informations de révocation ne soient acceptées que si elles ont été délivrées après le *best signature time*. Aucune valeur n'est fixée pour les contraintes «*RevocationFreshnessConstraints*» pour les certificats autres que le certificat de signature, y compris les certificats à l'appui des horodatages.

3) 4.3 Exigences relatives aux pratiques en matière de validation des signatures et de vérification des règles d'applicabilité

— REQ-4.3-02 Les applications de validation de signature doivent être conformes à l'ETSI TS 119 101 [13].

4) 4.4 Processus de vérification (des règles) de l'applicabilité technique

— REQ-4.4.2-03 Si l'une des vérifications prévues par REQ-4.4.2-01 échoue, alors:

— le processus s'arrête;

— la signature doit être techniquement considérée comme indéterminée, c'est-à-dire comme n'étant ni une signature électronique qualifiée de l'UE, ni un cachet électronique qualifié de l'UE;

— le résultat ci-dessus et les résultats de tous les processus intermédiaires doivent être pris en compte dans le rapport de vérification relatif aux règles d'applicabilité de la signature.

Journal officiel
de l'Union européenne

FR
Série L

2025/2160

28.10.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/2160 DE LA COMMISSION

du 27 octobre 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, les spécifications et les procédures applicables à la gestion des risques liés à la fourniture des services de confiance non 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 19 *bis*, paragraphe 2,

considérant ce qui suit:

(1) Les prestataires de services de confiance non qualifiés jouent un rôle important dans l'environnement numérique en fournissant des services de confiance qui facilitent les transactions électroniques sécurisées. Le règlement (UE) nº 910/2014 impose moins d'exigences réglementaires aux prestataires de services de confiance non qualifiés qu'aux prestataires de services de confiance qualifiés. Tous les prestataires de services de confiance sont néanmoins soumis à des exigences en matière de sécurité et de responsabilité, pour assurer une diligence appropriée, la transparence et la responsabilité quant à leurs activités et à leurs services.

(2) Les prestataires de services de confiance non qualifiés peuvent être considérés comme des entités importantes ou essentielles au sens de l'article 3 de la directive (UE) 2022/2555 du Parlement européen et du Conseil ([2]). À ce titre, le règlement d'exécution (UE) 2024/2690 de la Commission ([3]) établissant des exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité leur est applicable. Toutefois, le champ d'application des exigences énoncées à l'article 19 *bis*, paragraphe 1, point a), du règlement (UE) nº 910/2014 se rapporte aux procédures de gestion des risques concernant les risques juridiques, commerciaux et opérationnels ainsi que les autres risques directs ou indirects liés à la fourniture des services de confiance non qualifiés. Afin de compléter le cadre de gestion des risques énoncé dans le règlement d'exécution (UE) 2024/2690 et de permettre une approche cohérente de la gestion de tous les types de risques pertinents, il convient de définir les spécifications et procédures relatives à la gestion de ces risques par les prestataires de services de confiance non qualifiés. Les orientations fournies par l'Agence de l'Union européenne pour la cybersécurité (ENISA) ou les autorités nationales compétentes en vertu de la directive (UE) 2022/2555 peuvent aider les prestataires de services de confiance non qualifiés à concevoir et à mettre en œuvre des politiques de gestion des risques appropriées.

([1]) JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([3]) Règlement d'exécution (UE) 2024/2690 de la Commission du 17 octobre 2024 établissant des règles relatives à l'application de la directive (UE) 2022/2555 pour ce qui est des exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité et précisant plus en détail les cas dans lesquels un incident est considéré comme important, en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance (JO L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

(3) La présomption de conformité prévue à l'article 19 *bis*, paragraphe 2, du règlement (UE) nº 910/2014 ne devrait s'appliquer que lorsque les prestataires de services de confiance non qualifiés respectent les exigences énoncées dans le présent règlement. Les normes de référence visées à l'annexe devraient tenir compte des pratiques établies et être largement reconnues dans les secteurs concernés. Afin de garantir que les prestataires de services de confiance non qualifiés gèrent les risques juridiques, commerciaux et opérationnels ainsi que les autres risques directs ou indirects liés à la fourniture des services de confiance non qualifiés conformément à l'article 19 *bis*, paragraphe 1, du règlement (UE) nº 910/2014, lesdits prestataires devraient se conformer aux éléments des normes dont les références figurent dans l'annexe et aux exigences en matière de gestion des risques énoncées dans le présent règlement aux fins de la présomption de conformité.

(4) Si un prestataire de services de confiance non qualifié respecte les exigences énoncées dans le présent règlement d'exécution, les organes de contrôle devraient présumer que les exigences pertinentes du règlement (UE) nº 910/2014 sont respectées. Toutefois, un prestataire de services de confiance non qualifié peut toujours s'appuyer sur d'autres pratiques pour démontrer le respect des exigences du règlement (UE) nº 910/2014.

(5) Afin de garantir une prise en compte adéquate des risques identifiés, les politiques de gestion des risques appliquées par les prestataires de services de confiance non qualifiés devraient comprendre des procédures de documentation et d'évaluation des risques, ainsi que de définition, de sélection et de mise en œuvre de mesures de traitement du risque appropriées. La mise en œuvre des mesures de traitement du risque devrait faire l'objet d'un suivi continu. En ce qui concerne les informations que les prestataires de services de confiance non qualifiés enregistrent et conservent dans le cadre de leurs mesures de traitement du risque, lesdits prestataires devraient garantir l'intégrité et la confidentialité de ces données. En outre, afin de renforcer la transparence et de soutenir les activités de contrôle, les prestataires de services de confiance non qualifiés devraient publier les méthodes de vérification d'identité qu'ils appliquent. Étant donné que les risques identifiés ne peuvent pas tous être entièrement traités en les évitant, en les atténuant ou en les transférant à d'autres entités, tout risque résiduel devrait être approuvé par les organes de direction des prestataires de services de confiance non qualifiés. Les critères d'acceptation des risques résiduels devraient être justifiés de manière compréhensible.

(6) 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 ([4]), 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, les pratiques et les normes ou spécifications techniques et de suivre les meilleures pratiques sur le marché intérieur.

(7) Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([5]) et, le cas échéant, la directive 2002/58/CE du Parlement européen et du Conseil ([6]) s'appliquent à toutes les activités de traitement de données à caractère personnel au titre du présent règlement.

(8) 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 ([7]) et a rendu son avis le 8 août 2025 ([8]).

([4]) 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).

([5]) 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).

([6]) 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).

([7]) 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) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([8]) «EDPS Formal comments on the draft Implementing Regulation as regards specifications and procedures for the management of risks to the provision of non-qualified trust services» (Commentaires formels du CEPD sur le projet de règlement d'exécution en ce qui concerne les spécifications et les procédures applicables à la gestion des risques liés à la fourniture des services de confiance non qualifiés) | Contrôleur européen de la protection des données.

(9) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Normes de référence

Les normes de référence mentionnées à l'article 19 *bis*, paragraphe 2, du règlement (UE) nº 910/2014 figurent à l'annexe du présent règlement.

Article 2

Procédures de gestion des risques

1. Les procédures de gestion des risques visées à l'article 19 *bis*, paragraphe 1, du règlement (UE) nº 910/2014 déterminent clairement les services de confiance auxquels elles s'appliquent, sont spécifiques aux services de confiance concernés et sont approuvées par l'organe de direction du prestataire de services de confiance non qualifié.

2. Les procédures de gestion des risques comprennent au moins l'ensemble des éléments suivants:

a) le niveau global de tolérance au risque en fonction de la criticité et du niveau de sécurité requis des services de confiance, compte tenu des dernières évolutions technologiques;

b) les critères de risque pertinents, comprenant au moins la probabilité, l'incidence et le niveau du risque, compte tenu des renseignements sur les cybermenaces et des vulnérabilités;

c) une méthode pour l'identification et la documentation des risques liés à la fourniture des services de confiance, tenant compte de l'ensemble du champ d'activité du système d'information utilisé par le prestataire de services de confiance non qualifié, y compris les risques associés aux composantes du système ainsi qu'à toute partie active ou passive participant à la mise en œuvre du système ou à la fourniture des services de confiance;

d) un processus d'évaluation des risques identifiés sur la base des critères de risque visés au point b);

e) un processus d'identification, de hiérarchisation et de suivi continu de la mise en œuvre des mesures de traitement du risque appropriées;

f) un processus de suivi continu de la mise en œuvre des procédures de gestion des risques.

3. Les prestataires de services de confiance non qualifiés établissent des procédures appropriées et conservent des documents permettant de garantir la mise en œuvre des exigences énoncées dans la législation applicable.

4. Les prestataires de services de confiance non qualifiés établissent des procédures documentées et appropriées pour assurer le suivi des modifications législatives et réglementaires au niveau national et de l'Union susceptibles d'avoir une incidence sur la fourniture des services de confiance.

Article 3

Identification, documentation et évaluation des risques

Les prestataires de services de confiance non qualifiés identifient, documentent et évaluent tous les risques visés à l'article 19 *bis*, paragraphe 1, du règlement (UE) nº 910/2014 conformément aux procédures de gestion des risques visées à l'article 2, et notamment:

a) ils identifient les risques à l'égard des tiers;

b) ils identifient les points uniques de défaillance potentiels dans la fourniture des services de confiance;

c) ils évaluent les risques identifiés sur la base des critères de risque visés à l'article 2, paragraphe 2, point b).

Article 4

Mesures de traitement du risque

1. Conformément aux procédures visées à l'article 2, les prestataires de services de confiance non qualifiés planifient, documentent et mettent en œuvre des mesures de traitement du risque et effectuent notamment les tâches suivantes:

a) ils déterminent et hiérarchisent les mesures qu'il convient d'appliquer en matière de traitement des risques;

b) ils sélectionnent, approuvent et documentent les mesures de traitement du risque choisies, comprenant leurs exigences de sécurité et procédures opérationnelles, dans un plan de traitement du risque, et déterminent qui est responsable de la mise en œuvre des mesures de traitement du risque et à quel moment elles doivent être mises en œuvre;

c) ils suivent en continu la mise en œuvre des mesures de traitement du risque.

2. Le plan de traitement du risque visé au paragraphe 1, point b), indique les motifs justifiant l'acceptation des risques résiduels de manière compréhensible.

3. Dans le cadre des mesures de traitement du risque visées au paragraphe 1, les prestataires de services de confiance non qualifiés:

a) vérifient, le cas échéant, l'identité des utilisateurs du service de confiance, directement ou par l'intermédiaire d'un tiers, et publient des informations sur les méthodes de vérification d'identité utilisées;

b) enregistrent et conservent en lieu sûr, aussi longtemps que le prévoient le droit de l'Union ou le droit national, y compris après la cessation des activités du prestataire de services de confiance non qualifié, les informations suivantes, pour s'en servir comme preuve en justice et assurer la continuité du service:

— toutes les informations pertinentes recueillies dans le cadre du processus d'enregistrement et d'enrôlement des utilisateurs de services de confiance, y compris, le cas échéant, la vérification d'identité des utilisateurs,

— les données d'authentification assignées à l'utilisateur du service de confiance, le cas échéant, et

— tout changement de statut des certificats de clé publique ou de tout autre matériel cryptographique utilisé dans la fourniture du service de confiance;

c) veillent, le cas échéant, à ce que les données d'authentification assignées à l'utilisateur du service de confiance soient uniques.

4. Lorsqu'ils identifient, sélectionnent, approuvent et hiérarchisent les mesures de traitement du risque appropriées, les prestataires de services de confiance non qualifiés tiennent compte des éléments suivants:

a) les résultats de l'évaluation visée à l'article 3;

b) l'efficacité des mesures de traitement du risque;

c) les évaluations de la conformité;

d) les incidents importants;

e) le coût de la mise en œuvre par rapport à l'avantage escompté;

f) le classement approprié des actifs applicable;

g) l'analyse des incidences éventuelles des risques identifiés conformément à l'article 3 sur l'activité économique.

5. Les organes de direction des prestataires de services de confiance non qualifiés approuvent les risques résiduels qui subsistent après la mise en œuvre des mesures de traitement du risque prévues dans le plan de traitement du risque.

6. Les prestataires de services de confiance non qualifiés réexaminent, documentent et, le cas échéant, mettent à jour les résultats de l'évaluation des risques et le plan de traitement du risque à intervalles prédéfinis, et au moins une fois par an, ainsi qu'en cas de changements importants dans l'infrastructure, les opérations ou les risques, ou d'incidents importants.

7. Les prestataires de services de confiance non qualifiés veillent à la disponibilité, à l'intégrité et à la confidentialité des informations visées au paragraphe 3, point b).

Article 5

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 27 octobre 2025.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE

Liste des normes de référence applicables aux prestataires de services de confiance non qualifiés

Les exigences des clauses suivantes de la norme ETSI EN 319 401 V3.1.1 (2024-06) «Signatures électroniques et infrastructures de confiance — Exigences de politique générale des prestataires de service de confiance» s'appliquent:

5. Évaluation du risque
6. Politiques et méthodes
7.1 Organisation interne
7.2 Ressources humaines
7.3 Gestion des actifs
7.4 Contrôle d'accès
7.6 Sécurité physique et environnementale

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Digitalisation

TEXTE COORDONNÉ

Projet de loi relative à la mise en place du portefeuille européen d'identité numérique et portant mise en œuvre du règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique et modifiant la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques

Nous **Guillaume**, Grand-Duc de Luxembourg, Duc de Nassau,

Vu le règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique ;

Vu la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques et portant modification de

1. l'article 104 du Code civil ;
2. la loi modifiée du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales ;
3. la loi communale modifiée du 13 décembre 1988 ;
4. la loi électorale modifiée du 18 février 2003

et abrogeant

1. la loi modifiée du 22 décembre 1886 concernant les recensements de population à faire en exécution de la loi électorale et
2. l'arrêté grand-ducal du 30 août 1939 portant introduction de la carte d'identité obligatoire ;

Le Conseil d'État entendu ;

Vu l'adoption par la Chambre des Députés ;

Vu la décision de la Chambre des Députés du […] et celle du Conseil d'État du […] portant qu'il n'y pas lieu à second vote ;

Avons ordonné et ordonnons :

Chapitre 1er - Dispositions générales

Art. 1er. Objet et définitions

(1) La présente loi a pour objet de mettre en place le portefeuille européen d'identité numérique, tel que visé par le règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique, désigné ci-après par le terme « règlement (UE) n° 910/2014 ».

(2) Les termes et expressions définis à l'article 3 du règlement (UE) n° 910/2014 ont la même signification dans la présente loi.

Chapitre 2 – Compétences

Art. 2. Désignations des organismes compétents

(1) Le Centre des technologies de l'information de l'État, ci-après « CTIE », est désigné comme organisme chargé de fournir la solution nationale du portefeuille européen d'identité numérique, ci-après « le fournisseur » conformément à l'article 5*bis*, paragraphe 1er, du règlement (UE) n° 910/2014. Aux fins de la présente loi, la solution nationale du portefeuille européen d'identité numérique est dénommée ci-après « le portefeuille ».

~~(2) L'Office luxembourgeois d'accréditation et de surveillance est désigné comme organisme chargé de l'accréditation des organismes de certification, conformément à l'article 9, paragraphe 1er du règlement d'exécution (UE) 2024/2981 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne la certification des portefeuilles européens d'identité numérique.~~

(2) ~~(3)~~ L'Institut luxembourgeois de régulation est désigné comme organe de contrôle chargé du contrôle du fournisseur, ainsi que du portefeuille, conformément à l'article 46*bis*, paragraphe 1er, du règlement (UE) n° 910/2014.

(3) ~~(4)~~ Le membre du gouvernement ayant la digitalisation dans ses attributions assure la mission de point de contact unique, conformément à l'article 46*quater* du règlement (UE) n° 910/2014.

(4) ~~(5)~~ Le membre du gouvernement ayant la digitalisation dans ses attributions est désigné comme propriétaire des schémas nationaux de certification conformément à l'article 3, paragraphe 1er, du règlement d'exécution (UE) 2024/2981 de la Commission du 28 novembre 2024 précité.

(5) ~~(6)~~ Le **Commissariat du Gouvernement à la souveraineté des données** ~~Commissariat du gouvernement à la protection des données auprès de l'État~~ est désigné comme bureau d'enregistrement, conformément à l'article 3, paragraphe 3, du règlement d'exécution (UE) 2025/848 de la Commission du 6 mai 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne l'enregistrement des parties utilisatrices de portefeuille**, tel que modifié**.

(6) ~~(7)~~ Le CTIE est désigné comme autorité de certification chargée de délivrer des certificats d'accès aux parties utilisatrices enregistrées au registre des parties utilisatrices, conformément à l'article 7, paragraphe 1er, du règlement d'exécution (UE) 2025/848 précité.

(7) ~~(8)~~ Le CTIE est désigné comme autorité de certification chargée de délivrer des certificats d'enregistrement aux parties utilisatrices enregistrées au registre des parties utilisatrices, conformément à l'article 8, paragraphe 1er, du règlement d'exécution (UE) 2025/848 précité.

(8) Le traitement des données à caractère personnel par les autorités compétentes surnommées est autorisé dans la mesure où cela est nécessaire pour garantir le bon fonctionnement et l'intégrité du portefeuille, ainsi que pour la fourniture des services liés au portefeuille.

Chapitre 3 - Portefeuille et données d'identification personnelle

Art. 3. Données d'identification personnelle

(1) Le CTIE est l'organisme chargé de fournir les données d'identification personnelle des utilisateurs personnes physiques ~~et morales~~ aux fins de les associer à leur unité de portefeuille, conformément à l'article 5*bis*, paragraphe 5, point f)**,** du règlement (UE) n° 910/2014.

(2) Le CTIE fournit, à la demande, les données d'identification personnelle aux utilisateurs suivants du portefeuille :

- les personnes physiques ayant la nationalité luxembourgeoise,
- les personnes physiques résidant sur le territoire de l'État du Grand-Duché du Luxembourg et inscrites sur le registre national, dénommé ci-après « registre national des personnes physiques », tel que visé par l'article 4 de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques**.**~~;~~
- ~~les personnes morales ayant leur siège social sur le territoire de l'État du Grand-Duché du Luxembourg et inscrites au répertoire général, tel que visé par l'article 3 de la loi modifiée du 30 mars 1979 organisant l'identification numérique des personnes physiques ou morales.~~

(3) Les données d'identification personnelle d'un utilisateur personne physique, sont fournies par le CTIE sur base d'un accès direct au registre national des personnes physiques**, à l'exclusion du portrait numérique de l'utilisateur**. **Le portrait numérique est fourni par le CTIE sur base d'une communication préalable par l'utilisateur des informations nécessaires à cet effet, telles que requises et spécifiées par le CTIE le cas échéant.**

(4) Conformément à l'annexe, point 1er, tableau 1er**,** du règlement d'exécution (UE) 2024/2977 de la Commission du 28 novembre 2024 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les données d'identification personnelles et les attestations électroniques d'attributs délivrés aux portefeuilles européens d'identité numérique, **tel que modifié,** les données d'identification personnelle des utilisateurs personnes physiques sont **le portrait numérique et** l'ensemble des données énumérées à l'article 5, paragraphe 2, lettres a), d) et f)**,** de la loi modifiée du 19 juin 2013 précitée.

Afin de garantir que les données d'identification personnelle représentent de manière univoque la personne physique, conformément à l'article 5*bis*, paragraphe 5, point f)**,** du règlement (UE) n° 910/2014, il est ajouté aux données d'identification personnelle un numéro administratif personnel qui est associé au numéro d'identification au sens de l'article 1er de la

loi modifiée du 19 juin 2013 précitée, selon un processus informatisé standardisé qui protégera la confidentialité du numéro d'identification.

~~(5) Les données d'identification personnelle d'un utilisateur personne morale sont fournies par le CTIE sur base d'un accès direct au répertoire général.~~

~~(6) Conformément à l'annexe, point 2, tableau 3 du règlement d'exécution (UE) 2024/2977 précité, les données d'identification personnelle des utilisateurs personnes morales sont la dénomination sociale visée par l'article 3, paragraphe 2, point 2°, lettre a), ainsi que le numéro d'identité tel que visé par l'article 2 de la loi modifiée du 30 mars 1979 précitée.~~

(5) ~~(7)~~ Le CTIE associe les données d'identification personnelle fournies selon les procédures prévues au~~x~~ paragraphe~~s~~ 4 ~~et 6~~ à l'unité de portefeuille de l'utilisateur.

(6) ~~(8)~~ Le CTIE attribue un identifiant aux données d'identification personnelle de chaque utilisateur, et un identifiant à chaque unité de portefeuille. La création de ces deux identifiants est nécessaire afin de pouvoir associer l'identifiant des données d'identification personnelle à l'identifiant d'unité de portefeuille correspondant dans le registre dédié prévu au paragraphe suivant.

(7) ~~(9)~~ Conformément à l'article 5*bis*, paragraphe 14**,** du règlement n° 910/2014, le CTIE conserve, dans un registre dédié tenu séparément de tout autre registre contenant des données à caractère personnel :

- pour l'utilisateur personne physique, son numéro **administratif** personnel ~~administratif~~, l'identifiant de ses données d'identification personnelle**,** ~~et~~ l'identifiant de son unité de portefeuille **et son numéro d'identification au sens de l'article 1er de la loi modifiée du 19 juin 2013 précitée.**~~;~~
- ~~pour l'utilisateur personne morale, son numéro d'identité, l'identifiant de ses données d'identification personnelle et l'identifiant de son unité de portefeuille.~~

Sauf dispositions contraires, les données visées au présent paragraphe sont conservées pour la durée de 5 années après la fin de validité de l'unité de portefeuille pour prévenir tout dysfonctionnement résultant de la réutilisation de données invalidés. ~~La durée de conservation des données visées au présent paragraphe ne peut dépasser la durée de validité de l'unité de portefeuille.~~

(8) ~~(10)~~ Le CTIE est le responsable du traitement pour les opérations de traitement des données réalisées pour la fourniture des données d'identification personnelles et l'association au portefeuille dans le cadre du présent article au sens du 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).

(9) Les données d'identification personnelle au sens de l'article 3, point 3), du règlement (UE) n° 910/2014, si vérifiables, font foi de l'identité de la personne concernée et permettent de satisfaire à toute obligation d'identification indépendamment du caractère électronique ou non électronique de la procédure, sauf disposition légale contraire l'excluant expressément.

Art. 4. Enrôlement de l'utilisateur

Afin de garantir que les données d'identification personnelle émises vers le portefeuille d'un utilisateur, représentent l'utilisateur de manière univoque, conformément à l'article 5*bis*, paragraphe 5, point f)**,** du règlement (UE) n° 910/2014, ce dernier s'enrôle **:**

a) **soit** sur le guichet unique électronique visé à l'article 6 de la loi modifiée du 24 mai 2011 relative aux services dans le marché intérieur :

- par tout moyen d'identification électronique notifié de niveau de garantie élevé au sens de l'article 8, paragraphe 2, point c)**,** du règlement (UE) n° 910/2014, ou
- ~~**en s'identifiant à l'aide de sa carte d'identité ou de son passeport auprès de l'administration communale du lieu de résidence de l'utilisateur ou dans les locaux du guichet physique, ou**~~
- par tout moyen d'identification électronique notifié de niveau de garantie substantiel au sens de l'article 8, paragraphe 2, point b)**,** du règlement (UE) n° 910/2014, combiné avec les procédures d'enrôlement à distance supplémentaires conformes aux exigences établies par l'acte d'exécution (UE) 202**6**~~**X**~~/**798**~~**XXXX**~~ **de la Commission du 7 avril 2026 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les normes de référence et les spécifications applicables à l'enrôlement à distance des utilisateurs pour les portefeuilles européens d'identité numérique par des moyens d'identification électronique conformes au niveau de garantie substantiel combinés avec des procédures d'enrôlement à distance supplémentaires lorsque la combinaison répond aux exigences du niveau de garantie élevé,** prévu à l'article 5*bis*, paragraphe 24**,** du règlement (UE) n° 910/2014 ~~**;**~~**.**

b) **soit** en s'identifiant à l'aide de sa carte d'identité ou de son passeport auprès de l'administration communale du lieu de résidence de l'utilisateur**, auprès d'une mission diplomatique ou consulaire luxembourgeoise établie à l'étranger,** ou dans les locaux du guichet physique.

Art. 5. Code source de composants logiciels

Conformément à l'article 5*bis*, paragraphe 3**, deuxième phrase,** du règlement (UE) n° 910/2014, le code source de composants logiciels spécifiques autres que ceux installés sur les dispositifs utilisateurs **n'est pas** ~~**ne peut pas être**~~ divulgué lorsque ces composants sont liés à la garantie directe ou indirecte de la sécurité de l'infrastructure informatique de l'État **et il peut être dérogé à l'obligation prévue à l'article 5*bis*, paragraphe 3, première phrase, du règlement (UE) n° 910/2014 pour des raisons de coûts économiques disproportionnés ou d'inconvénients opérationnels majeurs** ~~**ou lorsque ceux-ci sont sujets aux droits de propriété intellectuelle**~~.

Art. 6. Suspension et révocation du portefeuille et de l'unité de portefeuille

(1) En application de l'article 5*bis*, paragraphe 9, lettre a)**,** du règlement (UE) n° 910/2014, la demande de révocation de la validité de l'unité de portefeuille de l'utilisateur se fait auprès du fournisseur par tous les moyens**, dont les délais et modalités pratiques sont fixés dans les conditions d'utilisation du portefeuille**. ~~**Ce dernier est tenu de révoquer la validité de cette unité de portefeuille endéans les vingt-quatre heures de la réception de la demande.**~~

(2) En application de l'article 5*bis*, paragraphe 9, lettre c)**,** du règlement (UE) n° 910/2014, la demande de révocation de la validité de l'unité de portefeuille en cas de décès de l'utilisateur ~~ou de cessation d'activité de la personne morale~~ se fait auprès du fournisseur par tous les moyens**, dont les délais et modalités pratiques sont fixés dans les conditions d'utilisation du portefeuille**. ~~Ce dernier est tenu de révoquer la validité de cette unité de portefeuille endéans les vingt-quatre heures de la réception de la demande.~~

~~(3) En application de l'article 5 sexies, paragraphe 1er du règlement (UE) n° 910/2014, le fournisseur suspend la fourniture et l'utilisation du portefeuille endéans les vingt-quatre heures à compter du moment où l'atteinte à la sécurité ou la compromission, a été constatée conformément à l'article 3, paragraphe 2 du règlement d'exécution (UE) 2025/847 de la Commission du 6 mai 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne les réactions aux atteintes à la sécurité des portefeuilles européens d'identité numérique.~~

~~(4)~~ **(3)** En cas de changement d'une ou plusieurs des données d'identification personnelle d'un utilisateur personne physique ~~ou morale~~, ces données d'identification personnelle sont automatiquement révoquées par le CTIE.

Art. 7. Statistiques

Le CTIE élabore des statistiques relatives au fonctionnement du portefeuille conformément à l'article 48*bis* du règlement (UE) n° 910/2014.

Chapitre 4 - Enregistrement des parties utilisatrices de portefeuille européen d'identité numérique

Art. 8. Enregistrement des parties utilisatrices de portefeuille européen d'identité numérique

(1) Le bureau d'enregistrement élabore la politique et les procédures nationales d'enregistrement conformément aux articles 4 et 6 du règlement d'exécution (UE) 2025/848 **de la Commission du 6 mai 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne l'enregistrement des parties utilisatrices de portefeuille, tel que modifié** ~~précité~~.

(2) Aux fins de l'enregistrement, les parties utilisatrices fournissent au bureau d'enregistrement, par voie électronique ou par moyens automatisés, les informations suivantes :

1° les informations requises par l'article 6 du règlement d'exécution (UE) 2025/848 précité ;

2° un extrait du casier judiciaire de la personne physique ou morale ou des représentants légaux de la personne, datant de moins d'un mois à la date du dépôt de la demande d'enregistrement ;

3° la preuve de la détention d'une autorisation d'établissement en cours de validité pour les parties utilisatrices soumises à l'obligation d'autorisation d'établissement prévue par la loi modifiée du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales ;

4° toutes autres informations nécessaires demandées par le bureau d'enregistrement aux fins des vérifications liées aux parties utilisatrices et à l'utilisation du portefeuille européen d'identité numérique par les parties utilisatrices conformément à l'article 5*ter* du règlement (UE) n° 910/2014 et au règlement d'exécution (UE) 2025/848 précité.

(3) En cas de recours à un intermédiaire agissant pour le compte de la partie utilisatrice, les données mentionnées au paragraphe précédent relatives à cet intermédiaire sont également communiquées au bureau d'enregistrement.

(4) La collecte des informations mentionnées au paragraphe 2, points 1° et 3°**,** peut être opérée par le bureau d'enregistrement par un accès direct :

1° au registre tenu par le membre du gouvernement ayant les autorisations d'établissement dans ses attributions, en vertu de l'article 32 la loi modifiée du 2 septembre 2011 précitée ;

2° au registre de commerce et des sociétés tenu en vertu de l'article 1er de la loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises ;

3° au registre national des personnes physiques ;

4° au répertoire général.

(5) Avec l'accord préalable de la partie utilisatrice, la collecte du bulletin n° 2 du casier judiciaire établi par la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire peut être opérée par le bureau d'enregistrement directement auprès du procureur général d'État.

Art. 9. Mise à la disposition du public des informations de la partie utilisatrice

Le bureau d'enregistrement **est l'organisme chargé de mettre** ~~**met**~~ les informations visées à l'annexe I du règlement d'exécution (UE) 2025/848 **de la Commission du 6 mai 2025 portant modalités d'application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil en ce qui concerne l'enregistrement des parties utilisatrices de portefeuille, tel que modifié** ~~**précité**~~ sur les parties utilisatrices enregistrées à la disposition du public en ligne**,** conformément à l'article 3, paragraphe 4**,** du règlement d'exécution (UE) 2025/848 précité.

Art. 10. Vérifications

(1) Le bureau d'enregistrement **est l'organisme chargé de procéder** ~~**procède**~~ aux vérifications liées aux parties utilisatrices et à l'utilisation du portefeuille par les parties utilisatrices conformément à l'article 5*ter* du règlement (UE) n°910/2014 et au règlement d'exécution (UE) 2025/848 précité.

(2) Aux fins des vérifications prévues au paragraphe 1er, le bureau d'enregistrement peut consulter par accès direct les fichiers mentionnés à l'article 8, paragraphe 4.

Lorsque des éléments démontrent un risque élevé d'utilisation illicite ou illégal du portefeuille européen d'identité numérique, un nouvel extrait du casier judiciaire peut être demandé à tout moment conformément aux modalités prévues à l'article 8.

(3) La responsabilité civile du bureau d'enregistrement pour des dommages individuels subis du fait de l'enregistrement d'une partie utilisatrice ne peut être engagée que s'il est prouvé que le dommage a été causé par une négligence grave dans le choix et l'application des moyens mis en œuvre pour l'accomplissement de la mission de service public du bureau d'enregistrement de l'alinéa précédent.

Art. 11. Suspension et annulation de l'enregistrement

~~(1)~~ En cas de soupçon d'une utilisation illicite ou illégal au regard du droit de l'Union européenne et du droit national du portefeuille européen d'identité numérique par une partie utilisatrice, une analyse peut être opérée par le bureau d'enregistrement.

~~(2) En cas d'utilisation non autorisée, frauduleuse ou illégale du portefeuille européen d'identité numérique par une partie utilisatrice, le bureau d'enregistrement :~~

~~- suspend ou annule l'enregistrement et l'inclusion des parties utilisatrices sur demande de l'organe de contrôle, conformément à l'article 9, paragraphe 1er du règlement d'exécution (UE) 2025/848 précité ;~~

~~- peut suspendre ou annuler, l'enregistrement et l'inclusion des parties utilisatrices de sa propre initiative conformément à l'article 9, paragraphe 2 du règlement d'exécution (UE) 2025/848 précité.~~

Art. 12. Système informatique

Le système informatique par lequel les accès prévus aux articles 8 et 10 sont opérés~~,~~ doit être aménagé de la manière suivante :

- l'accès aux fichiers est sécurisé moyennant une authentification forte ;
- les informations relatives aux personnes ayant procédé à la consultation ainsi que les informations consultées, la date et l'heure de la consultation sont enregistrées et conservées, afin que le motif du traitement puisse être retracé.

Art. 13. Recours

Un recours contre les décisions du bureau d'enregistrement peut être exercé devant le Tribunal administratif qui statue comme juge du fond.

Chapitre 5 - Attestations électroniques

Art. 14. Délivrance des attestations électroniques d'attributs par un organisme du secteur public

Le CTIE est désigné comme organisme du secteur public qui, pour le compte de l'organisme du secteur public responsable de la source authentique concernée peut émettre des attestations électroniques d'attributs, au sens de l'article 3 point 46, et de l'article 45*septies* du règlement (UE) n° 910/2014.

Sous réserve de la mise en place des démarches numériques respectives, pour les fins du traitement de la demande d'un utilisateur d'attestation électronique d'un attribut, le CTIE est autorisé à accéder aux données y nécessaires et à les traiter.

~~**L'ensemble des attestations électroniques d'attributs susceptibles d'être délivrées par un organisme du secteur public responsable d'une source authentique ou pour son compte, au sens de l'article 3 point 46, et de l'article 45 septies du règlement (UE) n° 910/2014, sont émises par l'organisme du secteur public responsable de la source authentique concernée ou par le CTIE.**~~

Chapitre 6 - Organe de contrôle

Art. 15. Attributions de l'organe de contrôle

(1) Dans la mesure nécessaire à l'accomplissement de ses missions en vertu de la présente loi, l'organe de contrôle peut demander la coopération des autorités sectorielles pertinentes, dont notamment la Commission de surveillance du secteur financier, le Commissariat aux Assurances ou l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services.

(2) L'obligation au secret professionnel prévue par l'article 15 de la loi modifiée du 30 mai 2005 portant : 1) organisation de l'Institut luxembourgeois de régulation ; 2) modification de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'État ne fait pas obstacle à l'échange d'informations confidentielles entre l'organe de contrôle, l'autorité de contrôle compétente en vertu du règlement (UE) n° 2016/679 précité, et le point de contact unique, dans le cadre et aux seules fins du règlement (UE) n° 910/2014, ainsi que de la présente loi et des mesures prises pour son exécution. En outre, l'obligation au secret professionnel des autorités sectorielles pertinentes ~~**prévue dans tout autre texte de loi similaire**~~ ne fait pas obstacle à cette coopération ou à l'échange d'informations confidentielles entre l'organe de contrôle et ces autorités dans le cadre et aux seules fins du règlement (UE) 910/2014, ainsi que de la présente loi et des mesures prises pour son exécution.

Art. 16. Frais de fonctionnement

L'organe de contrôle bénéficie d'une contribution financière à charge du budget de l'État afin de couvrir l'intégralité des frais de fonctionnement qui résultent de l'exercice des missions prévues par la présente loi.

Art. 17. Activités de contrôle

(1) L'organe de contrôle s'assure, au moyen d'activités de contrôle **en amont et en aval**~~**a priori et a posteriori**~~, que le fournisseur et le portefeuille qu'il fournit, satisfont aux exigences fixées dans le règlement (UE) n° 910/2014.

(2) Les activités de contrôle visées au paragraphe précédent doivent être effectives, proportionnées et dissuasives, compte tenu des circonstances de chaque cas.

(3) L'organe de contrôle, lorsqu'il accomplit les activités de contrôle **en amont et en aval** ~~**a priori et a posteriori**~~ visées au paragraphe 1er, a le pouvoir de soumettre le fournisseur à :

1° des inspections sur place et des contrôles à distance a priori et a posteriori, y compris des contrôles aléatoires effectués par des professionnels formés ;

2° des audits de conformité réguliers et ciblés réalisés par un organisme indépendant ou l'organe de contrôle ;

3° des audits ad hoc, notamment lorsqu'ils sont justifiés en raison d'un incident important ou d'une violation, par le fournisseur, de la présente loi ou du règlement (UE) n° 910/2014 ;

4° des demandes d'informations nécessaires à l'évaluation des mesures de gestion des risques adoptées par le fournisseur ;

5° des demandes d'accès à des données, à des documents et à toutes informations nécessaires à l'accomplissement de ses activités de contrôle ;

6° des demandes de preuves de la mise en œuvre des dispositions du règlement (UE) n° 910/2014, telles que les résultats des audits de conformité effectués par un auditeur qualifié et les éléments de preuve sous-jacents correspondants.

(4) Les résultats de tout audit sont mis à la disposition de l'organe de contrôle. Les coûts des audits effectués par un organisme indépendant sont à la charge du fournisseur, sauf lorsque l'organe de contrôle en décide autrement dans des cas dûment motivés.

(5) Lorsque l'organe de contrôle exerce ses pouvoirs en vertu du paragraphe 3, points 5°, 6° ou 7°, il mentionne la finalité de la demande et précise quelles sont les informations exigées.

Art. 18. Mesures d'exécution

(1) Au vu d'éléments de preuve, d'indications ou d'informations selon lesquels le fournisseur ne respecterait pas la présente loi ou le règlement (UE) n° 910/2014, l'organe de contrôle a le pouvoir de prendre une ou plusieurs des mesures d'exécution suivantes, le cas échéant, dans le cadre de mesures de contrôle **en aval** ~~**a posteriori**~~ :

1° d'adopter des instructions contraignantes, y compris en ce qui concerne les mesures nécessaires pour éviter un incident ou y remédier, ainsi que les délais pour mettre en œuvre ces mesures et rendre compte de cette mise en œuvre, ou une injonction exigeant du fournisseur qu'il remédie aux insuffisances constatées ou aux violations de la présente loi ou du règlement (UE) n° 910/2014 ;

2° d'ordonner au fournisseur de mettre un terme à un comportement qui viole la présente loi ou le règlement (UE) n° 910/2014 et de ne pas le réitérer ;

3° d'ordonner au fournisseur de garantir la conformité de ses mesures de gestion des risques ;

4° d'ordonner au fournisseur d'informer les personnes physiques ou morales à l'égard desquelles il fournit des services ou exerce des activités susceptibles d'être affectées par une non-conformité importante, de la nature de la non-conformité, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette non-conformité ;

5° d'ordonner au fournisseur de mettre en œuvre les recommandations formulées à la suite d'un audit de conformité ou d'un audit ad hoc dans un délai raisonnable ;

6° d'ordonner au fournisseur de rendre publics les aspects de violations de la présente loi ou du règlement (UE) n° 910/2014 de manière spécifique.

(2) L'organe de contrôle expose en détail les motifs des mesures d'exécution. Avant de prendre de telles mesures, il informe le fournisseur de ses conclusions préliminaires. Il laisse en outre à ce fournisseur un délai de 5 jours ouvrables pour communiquer ses observations, sauf dans des cas exceptionnels dûment motivés où cela empêcherait une intervention immédiate pour prévenir un incident ou y répondre.

(3) Les mesures d'exécution imposées au titre du paragraphe 1er sont uniquement appliquées jusqu'à ce que le fournisseur prenne les mesures nécessaires pour remédier aux insuffisances ou se conformer aux exigences de l'organe de contrôle à l'origine de l'application de ces mesures d'exécution.

(4) Lorsqu'il prend toute mesure d'exécution visée au paragraphe 1er, l'organe de contrôle respecte les droits de la défense et tient compte des circonstances propres à chaque cas et, au minimum, tient dûment compte :

1° de la gravité de la violation et de l'importance des dispositions enfreintes, les faits suivants, entre autres, devant être considérés en tout état de cause comme graves :
   a) les violations répétées ;
   b) le fait de ne pas notifier des incidents importants ou de ne pas y remédier ;
   c) le fait de ne pas pallier les insuffisances à la suite d'instructions contraignantes de l'organe de contrôle ;
   d) le fait d'entraver des audits ou des activités de contrôle ordonnées par l'organe de contrôle à la suite de la constatation d'une violation ;
   e) la fourniture d'informations fausses ou manifestement inexactes relatives aux mesures de gestion des risques ;

2° de la durée de la violation ;

3° de toute violation antérieure pertinente commise par le fournisseur ;

4° des dommages matériels, corporels ou moraux causés, y compris des pertes financières ou économiques, des effets sur d'autres services et du nombre d'utilisateurs touchés ;

5° du fait que l'auteur de la violation a agi délibérément ou par négligence ;

6° des mesures prises par le fournisseur pour prévenir ou atténuer les dommages matériels, corporels ou moraux ;

7° de l'application de mécanismes de certification approuvés.

(5) Lorsque les mesures d'exécution adoptées en vertu du paragraphe 1er sont inefficaces, l'organe de contrôle peut fixer un délai ne dépassant pas trois mois dans lequel le fournisseur est invité à prendre les mesures nécessaires pour pallier les insuffisances ou satisfaire aux exigences de l'organe de contrôle. Si la mesure demandée n'est pas prise dans le délai imparti, l'organe de contrôle a le pouvoir d'imposer une ou plusieurs sanctions visées à l'article 19.

Art. 19. Sanctions

(1) Si le fournisseur n'a pas remédié, dans le délai prévu à l'article 18, paragraphe 2, aux irrégularités étant à l'origine d'une ou de plusieurs des mesures d'exécution imposées, l'organe de contrôle peut frapper le fournisseur d'une ou de plusieurs des sanctions suivantes :

1° un avertissement ;

2° un blâme ;

3° une amende administrative, dont le montant est proportionné à la gravité du manquement et à l'ampleur du dommage sans pouvoir excéder 1.000.000 euros.

(2) Au moment de décider s'il y a lieu d'imposer une amende administrative et de décider de son montant, dans chaque cas d'espèce, il est dûment tenu compte, au minimum, des éléments prévus à l'article 18, paragraphe 4.

(3) Avant de prononcer une sanction visée au paragraphe 1er, l'organe de contrôle engage une procédure contradictoire dans laquelle le fournisseur a la possibilité de consulter le dossier et de présenter ses observations. Le fournisseur peut se faire assister ou représenter par une personne de son choix. À l'issue de la procédure contradictoire, l'organe de contrôle peut prononcer à l'encontre du fournisseur une ou plusieurs des sanctions visées au paragraphe 1er.

(4) Les décisions prises par l'organe de contrôle à l'issue de la procédure contradictoire sont motivées et notifiées au fournisseur.

(5) Contre les décisions visées au paragraphe 3, un recours en réformation est ouvert devant le tribunal administratif.

(6) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes administratives qui lui sont communiquées par l'organe de contrôle moyennant la transmission d'une copie des décisions de fixation. Le recouvrement est poursuivi comme en matière d'enregistrement.

Art. 20. Coopération en matière de protection des données à caractère personnel

(1) Lorsqu'il traite des incidents donnant lieu à des violations de données à caractère personnel, l'organe de contrôle coopère étroitement avec les autorités de contrôle en vertu du règlement (UE) 2016/679 précité, sans préjudice de la compétence et des missions de l'organe de contrôle.

(2) Lorsque l'organe de contrôle prend connaissance, dans le cadre de la supervision ou de l'exécution, du fait que la violation commise par le fournisseur à l'égard des obligations énoncées au règlement (UE) n° 910/2014 peut donner lieu à une violation de données à caractère personnel au sens de l'article 4, point 12°, du règlement (UE) 2016/679 précité, devant être notifiée en vertu de l'article 33 dudit règlement, il en informe sans retard injustifié les autorités de contrôle visées à l'article 55 ou 56 dudit règlement.

Chapitre 7 - Dispositions finales

Art. 21. Dispositions modificatives

La loi modifiée du 19 juin 2013 précitée est modifiée comme suit :

(1) A l'article 5, paragraphe 2 sont apportées les modifications suivantes :
- à la lettre n), le terme « et » est biffé ;
- à la lettre o), le signe de ponctuation « . » est remplacé par les termes « ; et »;
- une nouvelle lettre p), libellée comme suit, est ajoutée:

« p) pour les utilisateurs personnes physiques du portefeuille, le numéro administratif personnel contenu dans les données d'identification personnelle de l'unité de portefeuille européen d'identité numérique au sens de l'article 3, paragraphe 4, de la loi du […] relative à la mise en place du portefeuille européen d'identité numérique. ».

(2) A l'article 10, la lettre a) est remplacée par une nouvelle lettre a) libellée comme suit :
« a) la structure des numéros d'identification et des numéros administratifs personnels ; ».

(3) A l'article 11, alinéa 2, il est inséré entre le sixième tiret et le septième tiret, un nouveau tiret comprenant le libellé suivant :
« - d'un délégué du **Commissariat du Gouvernement à la souveraineté des données** ~~Commissariat du Gouvernement à la protection des données auprès de l'État~~, ».

(4) A l'article 12, paragraphe 2, la **43**ème phrase est remplacée par le libellé suivant :
« La carte d'identité contient en outre les éléments uniquement accessibles de manière électronique suivants :
a) le moyen d'authentification du titulaire de la carte d'identité, d'une durée de validité égale à la durée de la validité de la carte visée à l'article 15, paragraphe 2 ;
b) la clé privée relative au moyen visé à la lettre a) ;
c) le prestataire de service de certification agréé qui délivre le moyen visé à la lettre a) ;
d) l'information nécessaire à l'authentification de la carte et à la protection des données lisibles de manière électronique figurant sur la carte et à l'utilisation du certificat afférent ;
e) l'image faciale non codifiée du titulaire ;
f) le numéro d'identification ;
g) les deux empreintes digitales du titulaire. ».

(5) A l'article 12, paragraphe 2, **les** ~~la~~ **5ème, 6ème, et 7ème** ~~4ème~~ phrase**s** **sont** ~~est~~ remplacée**s** par le libellé suivant :
« ~~L'élément visé à la lettre a) de l'alinéa qui précède n'est pas activé pour les cartes d'identité délivrées aux majeurs incapables.~~ Pour les titulaires mineurs au moment de la délivrance de la carte d'identité, l'activation de l'élément visé à la lettre a) de

l'alinéa qui précède doit être autorisée par un parent exerçant l'autorité parentale ou par leur tuteur. ».

(6) Après l'article 15, paragraphe 1er, est insérée un nouveau paragraphe (1*bis*) comprenant le libellé suivant :

« (1*bis*) La personne réquisitionnée conformément au paragraphe 1er peut satisfaire à l'obligation de présentation de sa carte d'identité en présentant les données d'identification requises au moyen du portefeuille européen d'identité numérique visé par la loi du […] **relative à la mise en place du portefeuille européen d'identité numérique et portant mise en œuvre du règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique et modifiant la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques. »**

Art. 22. Entrée en vigueur

L'article 21, paragraphe 4 et paragraphe 5 entrent en vigueur le premier jour du vingt-quatrième mois qui suit celui de la publication de la présente loi au Journal officiel du Grand-Duché de Luxembourg.

Art. 23 ~~22~~. Intitulé de citation

La référence à la présente loi se fait sous la forme suivante : loi du […] relative à la mise en place du portefeuille européen d'identité numérique.

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Digitalisation

TEXTE COORDONNÉ

Loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques

Chapitre 1 – L'identification des personnes physiques, le registre national des personnes physiques et la carte d'identité

Section 1 – L'identification numérique des personnes physiques

Art. 1er.

(1) Un numéro d'identification est attribué :

a) à toute personne physique inscrite sur un registre communal des personnes physiques;
b) à toute personne physique enregistrée dans un fichier d'un organisme public tenu en vertu d'une disposition légale ou réglementaire d'employer ce numéro;
c) à toute personne physique de nationalité luxembourgeoise résidant à l'étranger et inscrite sur le registre national des personnes physiques, «désigné ci-après par les termes «registre national», auprès d'une mission diplomatique ou consulaire luxembourgeoise à l'étranger ou auprès du Centre des technologies de l'information de l'Etat, désigné ci-après par le terme «Centre».

(2) Le numéro d'identification, déterminé de telle façon qu'un même numéro ne puisse être attribué à plusieurs personnes et qu'une seule personne ne puisse se voir attribuer qu'un seul numéro, est composé de la date de naissance de la personne à laquelle il est attribué, d'une plage séquentielle unique par date de naissance et de deux numéros de contrôle.

Le numéro d'identification est automatiquement déterminé et alloué par l'application informatique du registre national à l'occasion de tout nouvel enregistrement d'une personne physique par les autorités compétentes et sous l'autorité du ministre ayant le Centre dans ses attributions, désigné ci-après par les termes « le ministre ».

(3) Au cas où un numéro attribué s'avère incomplet ou erroné, il est remplacé par un autre numéro. Le numéro de remplacement est notifié par lettre simple à la personne dont le numéro incomplet ou erroné a été remplacé ou, si la personne à laquelle le numéro est attribué est mineure d'âge non émancipée, à ses représentants légaux.

(4) Une personne reçoit un autre numéro d'identification à partir du moment où elle fait l'objet d'une adoption plénière. Le nouveau numéro est notifié par lettre simple à la personne ayant fait l'objet de cette adoption ou, si elle est mineure d'âge non émancipée, à ses représentants légaux.

Art. 2.

(1) Le numéro d'identification est enregistré sur la carte d'identité délivrée sur base des données figurant au registre national des personnes physiques et au registre des cartes d'identité.

(2) Les actes, documents et fichiers établis sur base des fichiers visés à l'article 1er, paragraphe 1er, lettre b) peuvent contenir le numéro d'identification, à condition que celui-ci soit réservé à l'usage à des fins administratives internes, aux relations entre l'Etat et les communes ou aux relations avec le titulaire du numéro.

(3) Les actes à transcrire ou à inscrire au bureau des hypothèques, en application de la loi modifiée du 26 juin 1953 concernant la désignation des personnes et des biens dans les actes à transcrire ou à inscrire au bureau des hypothèques, peuvent contenir le numéro d'identification.

(4) Les actes, documents et fichiers établis par les établissements hospitaliers tels que définis par l'article 1er de la loi modifiée du 28 août 1998 sur les établissements hospitaliers, par les établissements publics hospitaliers, par les laboratoires d'analyse de biologie médicale, par les médecins, les médecins-dentistes, les pharmaciens ou par les personnes visées par l'article 1er de la loi modifiée du 26 mars 1992 sur l'exercice et la revalorisation de certaines professions de santé peuvent contenir le numéro d'identification, à condition que celui-ci soit réservé à l'usage à des fins administratives internes ou aux relations avec le titulaire du numéro.

Le numéro d'identification doit figurer sur les ordonnances médicales et la correspondance des personnes mentionnées à l'alinéa qui précède avec les institutions de la sécurité sociale.

(5) Les actes, documents et fichiers établis par les commerçants et artisans, par les personnes exerçant une profession autre que celles mentionnées au paragraphe 4, par les personnes physiques ou par les personnes morales de droit privé, dans le cadre de la gestion de leur personnel, peuvent contenir le numéro d'identification.

(6) Les actes, documents et fichiers établis pour l'accomplissement d'une prestation de service demandée par la personne dont le numéro est utilisé et pour laquelle une disposition légale ou réglementaire exige la communication du numéro d'identification doivent contenir ce numéro.

Section 2 – L'identification biométrique des personnes physiques

Art. 3.

Il est procédé à l'identification d'une personne physique de nationalité luxembourgeoise sur base de données biométriques lisibles sur une carte d'identité.

Il y a lieu d'entendre par « données biométriques » des caractéristiques biologiques et morphologiques d'une personne physique transformées en une empreinte numérique.

Les données biométriques à collecter en vue de l'établissement d'une carte d'identité sont déterminées à l'article 12, paragraphe 2, alinéa 1er, lettres i) et j) et au paragraphe 2, lettre h) du même article.

Section 3 – Le registre national

Art. 4.

(1) Il est établi un registre national qui a pour finalités :

– l'identification des personnes physiques ;
– la mise à disposition de données de personnes physiques aux responsables des fichiers des organismes publics dans les limites des missions légales de ces organismes ou, à condition que les données soient anonymisées, à des fins statistiques ; et
– la préservation de l'historique de ces données à des fins administratives ou, à condition qu'elles soient anonymisées, à des fins statistiques.

(2) Le registre national garantit l'exactitude des données enregistrées sur base de pièces justificatives. Toute autre donnée y sera traitée comme donnée purement informative. Les données figurent dans un registre principal ou un registre d'attente conformément aux règles établies par le chapitre 2.

Le registre national sert de base à la production des documents de voyage, des pièces d'identité, des titres de séjour, des permis de conduire et d'autres documents administratifs. Il permet d'établir des certificats suivant la procédure prévue au chapitre 3.

Les responsables des fichiers visés à l'article 1er, paragraphe 1er, lettre b) qui ont accès au registre national ne peuvent plus exiger la production de certificats censés attester l'exactitude de données qualifiées d'exactes au titre de l'alinéa 1er, si ces données concernent des personnes ayant leur résidence habituelle au Luxembourg.

(3) Le registre national est divisé en un registre principal et un registre d'attente. Sont inscrites sur le registre principal, les personnes visées aux articles 24 et 25. Sont inscrites sur le registre d'attente, les personnes inscrites sur un registre communal d'attente conformément au chapitre 2 et les personnes dont les données nécessaires à l'inscription sur le registre national sont incomplètes ou non justifiées.

Art. 5.

(1) Le registre national contient les données des personnes physiques visées au paragraphe 1er de l'article 1er qui proviennent des registres communaux des personnes physiques, des registres tenus dans une mission diplomatique ou consulaire et des fichiers visés à l'article 1er, paragraphe 1er, point b).

(2) Le registre national comprend les données suivantes :

a) les nom et prénoms ;
b) le numéro d'identification ;
c) – la résidence habituelle, mentionnant la localité, la rue, le numéro d'immeuble, figurant ou à communiquer au registre national des localités et des rues, prévu par l'article 2, lettre g) de la loi modifiée du 25 juillet 2002 portant réorganisation de l'administration du cadastre et de la topographie, et le code postal ou la résidence habituelle, mentionnant le pays, la localité, la rue et le numéro d'immeuble à l'étranger ;

– le cas échéant, le numéro d'ordre établi en exécution de la loi modifiée du 19 mars 1988 sur la publicité foncière en matière de copropriété ;
– le cas échéant, toute précision supplémentaire quant à l'immeuble dans lequel se situe le logement et toute modification intervenue dans la situation de résidence ;
– le cas échéant, l'adresse de résidence de la personne en dehors de la commune où elle a sa résidence habituelle ;
– le cas échéant, l'adresse de référence telle que prévue par l'article 25 ;

d) les date et lieu de naissance;
e) la situation de famille;
f) la ou les nationalités ou le statut d'apatride ;
g) le statut de réfugié ou de protection subsidiaire ;
h) le sexe ;
i) pour les personnes mariées, séparées de corps ou liées par le partenariat en application de la loi modifiée du 9 juillet 2004 relative aux effets légaux de certains partenariats et pour les personnes veuves, le numéro d'identification pour autant que ce numéro ait été attribué, les noms, prénoms et dates de naissance des conjoints ou partenaires vivants ou prédécédés ;
j) les numéros d'identification des parents à l'égard desquels la filiation est établie, pour autant que ces numéros aient été attribués ;
k) les numéros d'identification des enfants à l'égard desquels la filiation est établie, pour autant que ces numéros aient été attribués ;
l) l'origine et les modifications des données enregistrées ;
m) les date et lieu de décès; […]
n) les titres de noblesse des membres de la famille grand-ducale ; ~~et~~
o) l'inscription sur les listes électorales constatant la qualité d'électeur pour les élections législatives, communales ou européennes~~.~~ **; et**
p) pour les utilisateurs personnes physiques du portefeuille, le numéro administratif personnel contenu dans les données d'identification personnelle de l'unité de portefeuille européen d'identité numérique au sens de l'article 3, paragraphe 4, de la loi du XXXXX relative à la mise en place du portefeuille européen d'identité numérique.

Art. 6.

Le Centre est chargé de toutes les opérations relatives à la gestion et à la tenue du registre national sous l'autorité du ministre.

Art. 7.

Le ministre s'assure que les données figurant au registre national soient traitées loyalement et licitement, qu'elles soient collectées pour les finalités prévues à l'article 4 et qu'elles ne soient pas traitées ou conservées ultérieurement de manière incompatible avec ces finalités.

Le ministre accorde l'accès au registre national en conformité avec les dispositions légales et réglementaires relatives au registre national et celles relatives à la législation sur la protection des données, après avoir demandé l'avis de la commission prévue à l'article 11.

Art. 8.

(1) Les autorités chargées de la communication des données au registre national par le biais d'inscriptions effectuées sur les fichiers visés à l'article 1er, paragraphe 1er, lettre b) transmettent par voie électronique au Centre les informations mentionnées à l'article 5, paragraphe 2. En cas d'impossibilité de transmettre les données par voie électronique, elles sont à transmettre sur support papier.

Les autorités précitées sont responsables de la conformité aux pièces justificatives de toute donnée inscrite ou modifiée et de toute information communiquée au Centre.

(2) Les données relatives à la conclusion ou à la dissolution d'un partenariat sont communiquées dans les formes prescrites au paragraphe 1er par l'autorité en charge de la tenue du répertoire civil.

Art.8*bis*

(1) L'administration communale ou le Centre délivre sur demande des personnes inscrites sur le registre principal du registre national des personnes physiques un certificat de résidence, sauf dans les cas visés par l'article 25 dans lesquels les personnes intéressées peuvent obtenir un certificat d'inscription à une adresse de référence.

(2) Un règlement grand-ducal fixe la forme et le contenu des certificats établis sur base des données figurant au registre national des personnes physiques. Parmi ces certificats figurent le certificat de résidence, le certificat d'inscription à une adresse de référence, le certificat de vie et le certificat d'inscription aux listes électorales.

Art. 9.

Les personnes autorisées à accéder aux données inscrites sur le registre national sont tenues de signaler au Centre toutes les erreurs dont elles ont connaissance.

Art. 10.

Un règlement grand-ducal fixe les modalités d'application de la présente loi, en ce qui concerne :

a) ~~**la structure des numéros d'identification;**~~ **la structure des numéros d'identification et des numéros administratifs personnels ;**
b) le traitement des dates à indiquer si celles-ci ne sont pas déterminables, voire pas déterminées, selon le calendrier grégorien;
c) l'agencement du registre national;
d) les modalités d'accès et de transmission des données du registre national.

Section 4 – La commission du registre national

Art. 11.

Il est institué sous l'autorité du ministre une commission du registre national dont les attributions sont les suivantes :

– analyser et régler dans la mesure du possible les difficultés d'application pratique pouvant résulter des dispositions légales et réglementaires relatives au registre national ;
– émettre les avis demandés par le ministre quant aux demandes d'accès au registre national ;
– faire le cas échéant des propositions au ministre afin d'améliorer la législation et la réglementation relatives au registre national ;
– émettre les avis demandés par le ministre quant aux lectures de cartes d'identité par des procédés de lecture informatique.

La commission est composée :
– d'un délégué du ministre,
– d'un délégué du ministre ayant les affaires intérieures dans ses attributions,
– d'un délégué du ministre ayant la justice dans ses attributions,
– d'un délégué du ministre ayant l'immigration dans ses attributions,
– d'un délégué du ministre ayant les affaires étrangères dans ses attributions,
– d'un délégué du Centre,
– **d'un délégué du Commissariat du Gouvernement à la souveraineté des données**~~**Commissariat du Gouvernement à la protection des données auprès de l'État**~~**,**
– d'un délégué de la Commission nationale pour la protection des données […],
– d'un représentant des communes délégué par le Syndicat des Villes et Communes Luxembourgeoises (Syvicol).

Pour chaque membre effectif, il est nommé un membre suppléant.

Le ministre nomme les membres effectifs et suppléants pour un mandat renouvelable de cinq ans.

En cas de vacance le membre nommé en remplacement achèvera le mandat de son prédécesseur.

Un règlement grand-ducal détermine le fonctionnement de la commission du registre national.

Section 5 – La carte d'identité

Art. 12.

(1) L'État délivre par l'intermédiaire des administrations communales ou par l'intermédiaire du Centre une carte d'identité à chaque Luxembourgeois résidant au Grand-Duché de Luxembourg et inscrit sur le registre national des personnes physiques.

L'Etat délivre par l'intermédiaire des missions diplomatiques ou consulaires luxembourgeoises établies à l'étranger ou par l'intermédiaire des missions diplomatiques ou consulaires belges en vertu

de la Convention entre le Grand-Duché de Luxembourg et la Belgique relative à la coopération dans le domaine consulaire du 30 septembre 1965 ou encore par tout autre intermédiaire en vertu d'un accord bilatéral conclu au préalable ou par l'intermédiaire du Centre, une carte d'identité aux Luxembourgeois résidant à l'étranger, inscrits sur le registre national par une mission diplomatique ou consulaire luxembourgeoise à l'étranger et ayant demandé la délivrance d'une carte d'identité.

(2) La carte d'identité est établie sur base des données inscrites sur le registre national et sur le registre des cartes d'identité. Elle contient des données à caractère personnel visibles à l'œil nu et, à l'exception de la donnée visée à la lettre i) du présent alinéa, lisibles de manière électronique, à savoir :

a) le nom et, sur demande du titulaire, le nom du conjoint vivant ou prédécédé;
b) le prénom ou les deux ou trois premiers prénoms;
c) la nationalité;
d) la date de naissance;
e) le sexe;
f) le lieu de la délivrance de la carte;
g) la date de début et de fin de validité de la carte;
h) la dénomination et le numéro de carte;
i) la photographie numérisée du titulaire;
j) la signature numérisée du titulaire et
k) la signature numérisée du ministre ayant les Affaires intérieures dans ses attributions.

Les cartes d'identité des membres de la famille grand-ducale contiennent également leurs titres de noblesse.

~~**La carte d'identité contient en outre les informations uniquement lisibles de manière électronique suivantes:**~~

~~**a) les moyens d'authentification et de signature du titulaire de la carte d'identité si celui-ci en a fait la demande ;**~~
~~**b) le cas échéant, les clés privées relatives aux moyens visés à la lettre a) ;**~~
~~**c) le cas échéant, le prestataire de service de certification agréé qui délivre les moyens visés à la lettre a) ;**~~
~~**d) l'information nécessaire à l'authentification de la carte et à la protection des données lisibles de manière électronique figurant sur la carte et à l'utilisation des certificats qualifiés et afférents ;**~~
~~**e) l'image faciale non codifiée du titulaire ;**~~
~~**f) […]**~~
~~**g) le numéro d'identification ; et**~~
~~**h) les deux empreintes digitales du titulaire.**~~

La carte d'identité contient en outre les éléments uniquement accessibles de manière électronique suivants :

a) le moyen d'authentification du titulaire de la carte d'identité, d'une durée de validité égale à la durée de la validité de la carte visée à l'article 15, paragraphe 2 ;
b) la clé privée relative au moyen visé à la lettre a) ;
c) le prestataire de service de certification agréé qui délivre le moyen visé à la lettre a) ;

d) **l'information nécessaire à l'authentification de la carte et à la protection des données lisibles de manière électronique figurant sur la carte et à l'utilisation du certificat afférent ;**
e) **l'image faciale non codifiée du titulaire ;**
f) **le numéro d'identification ;**
g) **les deux empreintes digitales du titulaire.**

~~**Le titulaire de la carte d'identité peut demander l'activation des éléments visés aux lettres a) et b) de l'alinéa qui précède. Toutefois, ces éléments ne peuvent pas être activés pour les cartes d'identité délivrées aux personnes âgées de moins de quinze ans ou aux majeurs incapables. Pour les titulaires mineurs âgés de quinze ans au moins au moment de la délivrance de la carte d'identité, l'activation des éléments visés aux lettres a) et b) de l'alinéa qui précède doit être demandée par un parent exerçant l'autorité parentale ou par leur tuteur.**~~

~~**L'élément visé à la lettre a) de l'alinéa qui précède n'est pas activé pour les cartes d'identité délivrées aux majeurs incapables.**~~ **Pour les titulaires mineurs au moment de la délivrance de la carte d'identité, l'activation de l'élément visé à la lettre a) de l'alinéa qui précède doit être autorisée par un parent exerçant l'autorité parentale ou par leur tuteur.**

Les enfants de moins de douze ans sont exemptés de l'obligation de donner leurs empreintes digitales.

Art. 13.

Au moment de la remise de la carte d'identité, le titulaire ou son représentant légal peut demander à pouvoir lire les données électroniques qui sont enregistrées sur la carte d'identité. Il peut demander la communication des données en suivant la procédure prévue par respectivement l'article 36 ou l'article 37. La rectification des données ne peut se faire que moyennant rectification des données du registre national conformément à la procédure prévue par l'article 37.

Art. 14.

Tout procédé de lecture informatique des cartes d'identité doit faire l'objet d'une autorisation du ministre, l'avis de la commission du registre national ayant été demandé.

Art. 15.

(1) La carte d'identité est obligatoire à partir de l'âge de quinze ans pour les ressortissants luxembourgeois qui résident habituellement dans une commune sur le territoire du Luxembourg et est exigible à toute réquisition de la Police grand-ducale. Elle est délivrée sur demande aux Luxembourgeois qui résident à l'étranger et aux Luxembourgeois âgés de moins de quinze ans.

(1*bis*) La personne réquisitionnée conformément au paragraphe 1er peut satisfaire à l'obligation de présentation de sa carte d'identité en présentant les données d'identification requises au moyen du portefeuille européen d'identité numérique visé par la loi du […] **relative à la mise en place du**

portefeuille européen d'identité numérique et portant mise en œuvre du règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique et modifiant la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques.

(2) Les cartes d'identité délivrées aux Luxembourgeois âgés, au moment de la délivrance, de quinze ans ou plus, sont valables pour une durée de dix ans. Les cartes d'identité délivrées aux Luxembourgeois âgés, au moment de la délivrance, de moins de quinze ans mais de quatre ans ou plus sont valables pour une durée de cinq ans. Les cartes d'identité délivrées aux Luxembourgeois ayant, au moment de la délivrance, moins de quatre ans sont valables pour une durée de deux ans.

(3) Une taxe de chancellerie est due par le titulaire de la carte d'identité, ou son représentant légal, au moment de la demande de la carte d'identité.

(4) Un règlement grand-ducal détermine :

- la forme, le modèle, les procédures de demande et de délivrance des cartes d'identité ;
- le montant de la taxe de chancellerie et les modalités de paiement ;
- les procédures et formalités de fabrication des cartes d'identité ; et
- les obligations du titulaire de la carte d'identité en cas de vol, de perte ou de détérioration de la carte.

Art. 16.

(1) Il est établi un registre des cartes d'identité qui a pour finalités de collecter les demandes de cartes d'identité, de permettre la délivrance des cartes d'identité sur base des données reprises du registre national et de répertorier les cartes d'identité émises.

Sous réserve du paragraphe 3, le registre des cartes d'identité contient pour chaque titulaire de carte d'identité les données énumérées à l'article 12, à l'exception de celles énumérées au paragraphe 2, alinéa 3, aux lettres a), b), c), d) et e). Le registre contient également les données suivantes :

a) le numéro de la demande, la date de la demande, la date de l'émission, le cas échéant la date de la perte, du vol ou de la détérioration de la carte d'identité;
b) la date de la délivrance de la carte d'identité;
c) le numéro de séquence de fabrication de la carte;
d) l'information que la carte d'identité est valable, périmée, perdue, volée ou détériorée et, dans ce dernier cas, la raison; et
e) la date de la dernière mise à jour des données.

(2) Les fonctionnaires et employés publics qui saisissent ou traitent les données relatives aux cartes d'identité ont d'office accès au registre des cartes d'identité et au registre national pour ce qui est des données nécessaires à l'établissement d'une carte d'identité.

(3) Les données biométriques ne sont conservées que pendant une durée de deux mois après la délivrance d'une carte d'identité et sont, à l'expiration de ce délai, automatiquement et irréversiblement supprimées.

Chapitre 2 – Les registres communaux des personnes physiques

Section 1 – Objet et champ d'application

Art. 17.

Chaque commune tient un registre des personnes physiques, ci-après le « registre communal », divisé en un registre principal et un registre d'attente.

Le registre communal est distinct du registre de l'état civil.

Art. 18.

Le registre communal est destiné à la collecte des données des personnes physiques qui établissent leur résidence habituelle sur le territoire d'une commune, ainsi qu'à la collecte des données de toute autre personne visée par les dispositions de la présente loi.

Ces données servent de base à l'exécution de la loi électorale modifiée du 18 février 2003, de l'article 5*ter* de la loi communale modifiée du 13 décembre 1988 ainsi qu'à l'organisation des services d'une commune.

Toutes les personnes inscrites sur le registre communal sont prises en compte lors du recensement de la population à faire en exécution de l'article 5*ter* de la loi communale modifiée du 13 décembre 1988 et pour toute fixation du chiffre de la population.

Section 2 – La tenue du registre communal

Art. 19.

Le bourgmestre est chargé de la tenue du registre communal. Il peut déléguer, sous sa surveillance et sa responsabilité, la tenue du registre communal à un ou plusieurs agents communaux, désignés ci-après par les termes « l'agent délégué ». Par agent communal, il y a lieu d'entendre un fonctionnaire ou employé communal, ainsi qu'un salarié à tâche principalement intellectuelle au service de la commune. La décision portant délégation est transmise […]au ministre ayant les Affaires intérieures dans ses attributions qui la transmet au ministre.

Le bourgmestre et l'agent délégué ont accès au registre national pour consulter et utiliser, dans les limites des finalités du registre national et du registre communal, les données énumérées à l'article 5 paragraphe 2 de la présente loi, ainsi que l'historique de ces données.

Art. 20.

Le registre communal est en permanence tenu à jour. Le bourgmestre s'assure que les données ne soient collectées que dans le but de remplir les finalités de l'article 18.

Section 3 – Les déclarations d'arrivée

Art. 21.

(1) Toute personne qui établit sa résidence habituelle sur le territoire d'une commune est tenue d'en faire la déclaration auprès de cette commune.

Toute personne qui transfère sa résidence habituelle dans une autre commune luxembourgeoise est tenue d'en faire la déclaration auprès de cette commune.

Toute personne qui transfère sa résidence habituelle à l'intérieur d'une même commune est tenue d'en faire la déclaration auprès de cette commune.

Toute personne qui transfère sa résidence habituelle à l'étranger est tenue de faire une déclaration de départ auprès de la commune où elle est inscrite avant son départ.

(2) La déclaration d'arrivée doit être effectuée dans les huit jours de l'occupation de la nouvelle résidence et, en cas de transfert de la résidence habituelle à l'étranger, la déclaration de départ doit être effectuée au plus tard la veille du départ. L'inscription prend effet au jour de l'occupation de la nouvelle résidence sans que cette date puisse être antérieure à la date où la déclaration d'arrivée a été effectuée. La radiation suite au transfert de la résidence habituelle à l'étranger prend effet au jour de la date de départ indiquée par la personne concernée.

(3) La déclaration doit être effectuée par la personne concernée ou par un représentant qui est son conjoint ou son partenaire avec lequel elle réside habituellement, son tuteur, son curateur, son administrateur légal, son administrateur ad hoc ou son mandataire spécial sur base d'un document d'identité en cours de validité et du titre sur base duquel il agit. Les mineurs d'âge non émancipés sont représentés par celui de leurs parents qui exerce l'autorité parentale ou par le tuteur.

Pour une personne détenue dans un établissement pénitentiaire qui ne dispose plus d'une résidence habituelle, la déclaration peut être effectuée, avec l'accord de la personne concernée, par le directeur de l'établissement concerné ou un membre du personnel délégué par le directeur à cette fin.

Pour une personne admise dans un des établissements visés à l'article 23, paragraphe 2, lettre a), la déclaration peut être effectuée, avec l'accord de la personne concernée, par le directeur de l'établissement concerné ou un membre du personnel délégué par le directeur à cette fin.

(4) Lorsqu'un mineur d'âge non émancipé quitte la résidence habituelle de ses parents, de celui de ses parents qui exerce l'autorité parentale ou de son tuteur et fixe sa résidence habituelle ailleurs, la déclaration doit être faite par celui de ses parents qui exerce l'autorité parentale ou par son tuteur. Il

en va de même lors de tout changement de résidence ultérieur jusqu'à sa majorité ou son émancipation.

(5) Toute déclaration d'arrivée et de départ doit être signée par la personne qui y a procédé.

Art. 22.

(1) Une personne est présumée avoir sa résidence habituelle au lieu où elle réside de façon réelle et continue.

La personne qui, pour des raisons autres que celles énumérées à l'article 23, réside pour une durée de moins de six mois sur douze sur le territoire d'une commune, n'est pas inscrite ou maintenue inscrite sur le registre communal.

Par exception, la personne qui pour des raisons professionnelles est dans l'impossibilité d'avoir une résidence habituelle sur le territoire luxembourgeois ou à l'étranger, mais qui a pourtant une résidence sur le territoire luxembourgeois est inscrite sur le registre principal de la commune de sa résidence. Cette personne déclare à la commune de sa résidence son absence pour des raisons professionnelles appuyée par une attestation de son employeur ou du Centre commun de la Sécurité sociale. Cette attestation est à verser chaque année au cours du mois de janvier. L'adresse à mentionner au registre communal est l'adresse à laquelle la personne concernée réside en dehors de ses déplacements professionnels.

Le mineur d'âge non émancipé, dont les parents divorcent ou sont divorcés et dont la résidence a été fixée en alternance au domicile de chacun de ses parents, est inscrit sur le registre communal d'une des communes dans laquelle réside habituellement l'un de ses parents. Le choix de la commune d'inscription est effectué d'un commun accord entre les parents. A défaut d'accord, les parents peuvent saisir le juge compétent de la question. En attendant un jugement définitif, le mineur d'âge non émancipé demeure inscrit sur le registre de la commune où il a résidé habituellement jusqu'au prononcé du divorce de ses parents.

(2) En cas de doute sur la réalité de l'existence d'une résidence habituelle sur le territoire de la commune, le bourgmestre ou l'agent délégué inscrit la personne dont la déclaration est remise en question, sur le registre d'attente et lui demande de prouver les faits remis en cause.

La preuve de la résidence habituelle peut être établie sur la base de tous documents émanant d'un service public ou des mentions figurant dans les registres, documents, bordereaux imposés par la loi ou consacrés par l'usage et régulièrement tenus ou établis.

La preuve de la résidence habituelle peut également être établie à partir d'autres éléments, tels que le lieu rejoint régulièrement après les occupations professionnelles, le lieu de fréquentation scolaire des enfants, les consommations en énergie domestique, les frais de téléphone, le contrat de bail, l'accord du propriétaire ou de l'occupant du logement, la résidence habituelle du conjoint, du partenaire ou de tout autre membre de la famille.

A défaut de preuve suffisante, le bourgmestre ou l'agent délégué demande à la Police grand-ducale d'effectuer une enquête et de lui faire parvenir un rapport écrit dans un délai de deux mois à partir de la demande d'enquête.

Si le rapport de l'enquête réalisée par la Police grand-ducale n'a pas été remis dans les délais, le bourgmestre ou l'agent délégué procède, sans préjudice des dispositions des articles 27 et 31, à l'inscription du déclarant sur le registre principal.

Le bourgmestre ou l'agent délégué décide, dans les huit jours de l'obtention du rapport de l'enquête menée par la Police grand-ducale, soit d'une inscription sur le registre principal, soit d'un maintien sur le registre d'attente, soit d'une radiation du registre communal.

En cas de décision d'inscription sur le registre principal, celle-ci est notifiée à la personne qui a demandé l'inscription au lieu de sa résidence habituelle.

En cas de maintien de l'inscription sur le registre d'attente pour une autre raison énumérée par la présente loi, cette décision motivée de maintien est notifiée à la personne qui a demandé l'inscription à l'adresse qu'elle a indiquée comme résidence habituelle.

En cas de radiation du registre communal, la décision motivée de radiation est notifiée à la personne qui a demandé l'inscription à l'adresse qu'elle a indiquée comme résidence habituelle.

Art. 23.

(1) L'absence temporaire du territoire de la commune ne constitue pas un changement de résidence habituelle.

(2) Sont considérés comme temporairement absents :

a) les personnes admises dans les hôpitaux, les établissements hospitaliers spécialisés, les foyers de réadaptation, les établissements de convalescence, les établissements de cures thermales, les centres de diagnostic et autres établissements publics ou privés destinés à recevoir des malades, les centres intégrés pour personnes âgées, les maisons de repos et de soins, les hôpitaux ou parties d'hôpitaux assimilés à des maisons de repos et de soins, tout autre établissement médico-social assurant un accueil de jour et de nuit, ainsi que les établissements psychiatriques;
b) les personnes absentes du territoire luxembourgeois pour moins d'un an pour des raisons de santé ou de tourisme;
c) les personnes qui effectuent de manière exceptionnelle et unique, pour des raisons professionnelles, une mission déterminée en dehors du territoire luxembourgeois;
d) les personnes qui résident, pour des raisons d'études, en dehors du lieu de leur résidence habituelle et qui sont couverts par la sécurité sociale de leurs parents;
e) les personnes détenues dans les établissements pénitentiaires;
f) les membres de l'Armée luxembourgeoise, de la Police grand-ducale et de l'Administration des douanes et accises détachés à l'étranger, soit auprès d'un organisme international ou supranational, soit auprès d'une base militaire en pays étranger;
g) les agents diplomatiques, les membres du personnel administratif et technique des missions diplomatiques et consulaires luxembourgeoises, les fonctionnaires consulaires et les employés consulaires de carrière ainsi que leur conjoint ou partenaire au sens de la loi modifiée du 9 juillet 2004 relative aux effets légaux de certains partenariats et leurs descendants et
h) les personnes envoyées par le ministre compétent en mission de coopération pour la durée de leur mission de coopération.

(3) Ne sont pas considérées comme temporairement absentes et sont inscrites sur le registre communal de la commune où elles ont leur résidence habituelle ou de la commune sur le territoire de laquelle se situe l'établissement où elles résident habituellement :

a) les personnes visées au paragraphe 2 lettre a) du présent article qui demandent l'inscription ou qui ne disposent plus de logement dans leur commune d'origine;
b) les personnes visées au paragraphe 2 lettre d) du présent article qui demandent l'inscription sur le registre communal de la même commune, d'une autre commune ou à l'étranger; et
c) les personnes visées au paragraphe 2 lettre e) du présent article qui ne disposent plus de logements.

Section 4 – Les inscriptions au registre communal

Art. 24.

Sont inscrits sur le registre principal, lorsqu'ils établissent leur résidence habituelle sur le territoire de la commune et sous réserve des articles 27 et 31 :

a) les Luxembourgeois;
b) les citoyens de l'Union européenne, les ressortissants des autres Etats parties à l'Accord sur l'Espace économique européen et ceux de la Confédération suisse, ainsi que les membres de leur famille, quelle que soit leur nationalité, qui bénéficient d'un droit au séjour en vertu des dispositions prévues par la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration; l'établissement de l'attestation d'enregistrement ou de la demande en obtention d'une carte de séjour de membre de famille donne automatiquement lieu à l'inscription sur le registre principal; […]
c) les ressortissants de pays tiers disposant d'un titre de séjour valable en vertu de la loi modifiée du 29 août 2008 précitée ;
d) le personnel de l'Union européenne ou d'une autre institution internationale qui ne jouit pas du statut diplomatique, ainsi que les membres de leur famille auxquels une carte de légitimation est délivré par le ministre ayant les Affaires étrangères dans ses attributions ; et
e) le personnel administratif et technique des missions diplomatiques et consulaires résidentes, ainsi que les membres de leur famille auxquels une carte de légitimation est délivrée par le ministre ayant les Affaires étrangères dans ses attributions.

Art. 25.

(1) Peuvent demander à être inscrits sur le registre principal les Luxembourgeois et, après une durée de résidence et d'affiliation à la sécurité sociale du Grand-Duché de Luxembourg de cinq années au moins, les citoyens de l'Union européenne ainsi que les ressortissants d'un des autres États parties à l'Accord sur l'Espace économique européen ou de la Confédération suisse qui n'ont pas de résidence au Luxembourg ou à l'étranger qu'ils pourraient occuper de façon habituelle. Ils sont inscrits à une adresse de référence s'ils sont présumés présents sur le territoire de la commune pendant une durée qui dépasse six mois sur une période de douze mois.

Par adresse de référence, il y a lieu d'entendre l'adresse habituelle d'une personne morale œuvrant dans les domaines social, familial et thérapeutique, dûment agréée conformément à la loi modifiée

du 8 septembre 1988 réglant les relations entre l'Etat et les organismes œuvrant dans les domaines social, familial et thérapeutique, à laquelle peuvent être adressés le courrier et les documents administratifs, et être signifiés ou notifiés les documents judiciaires en vue de leur transmission effective à leur destinataire.

A défaut d'indication d'une adresse réelle d'une personne morale visée à l'alinéa 2 par le demandeur à l'inscription sur le registre principal, l'adresse de l'office social territorialement compétent pour la commune tenant le registre principal sur lequel cette personne demande à être inscrite constitue l'adresse de référence.

Les personnes inscrites à une adresse de référence doivent se présenter tous les six mois à l'administration communale du lieu de leur inscription.

(2) Les détenus dans les établissements pénitentiaires peuvent bénéficier d'une adresse de référence auprès d'une personne physique ou morale avec l'accord écrit de celle-ci et à condition que cet accord comporte l'engagement que le détenu pourra établir sa résidence à l'adresse indiquée après avoir purgé sa peine privative de liberté.

(3) Les bénéficiaires d'une protection internationale en vertu des articles 46 ou 51 de la loi du 18 décembre 2015 relative à la protection internationale et à la protection temporaire demandent à être inscrits sur le registre principal.

Si des dispositions légales ou réglementaires empêchent une inscription sur le registre principal, ils peuvent bénéficier d'une adresse de référence. Par adresse de référence, il y a lieu d'entendre l'adresse locale ou nationale de l'Office luxembourgeois de l'accueil et de l'intégration ou d'une personne morale œuvrant dans les domaines social, familial et thérapeutique, dûment agréée conformément à la loi modifiée du 8 septembre 1998 réglant les relations entre l'Etat et les organismes œuvrant dans les domaines social, familial et thérapeutique. Ils sont dans ces cas inscrits à une adresse de référence s'ils sont présumés présents sur le territoire de la commune et à condition de disposer d'un accord écrit de l'Office luxembourgeois de l'accueil et de l'intégration ou de la personne morale.

A défaut d'indication d'une adresse visée à l'alinéa 2 par le demandeur à l'inscription sur le registre principal, l'adresse de l'office social territorialement compétent pour la commune tenant le registre principal sur lequel cette personne demande à être inscrite constitue l'adresse de référence.

Les personnes inscrites à une adresse de référence doivent se présenter tous les six mois à l'administration communale du lieu de leur inscription.

Art. 26.

[…]

Art. 27.

(1) Sont inscrits sur le registre d'attente :

a) les personnes qui sollicitent une inscription sur le registre communal, mais dont l'endroit où elles entendent établir leur résidence habituelle ne saurait servir à cette fin parce qu'une disposition légale ou réglementaire y interdit la résidence habituelle pour des motifs de sécurité, de salubrité, d'urbanisme ou d'aménagement du territoire;
b) les personnes dont la réalité ou la continuité de la résidence habituelle déclarée est soumise à une vérification conformément à l'article 22, paragraphe 2 ;
c) les personnes inscrites au registre national par un responsable d'un fichier visé à l'article 1er, paragraphe 1er, lettre b) à une adresse établie dans une commune luxembourgeoise et qui n'ont pas encore effectué leur déclaration d'arrivée dans la commune de la résidence indiquée au registre national ;
d) les ressortissants de pays tiers qui font une déclaration d'arrivée pour un séjour jusqu'à trois mois en application de l'article 36 ou pour un séjour de plus de trois mois en application de l'article 40, paragraphe 1er de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration ;
e) les ressortissants de pays tiers qui sont titulaires d'une attestation en cours de validité telle que prévue par les articles 6, paragraphe 5 ou 62 de la loi modifiée du 5 mai 2006 relative au droit d'asile et à des formes complémentaires de protection ;
f) les étrangers qui ont reçu une décision de retour telle que visée à l'article 3, lettre h) de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration ou une décision d'éloignement telle que visée à l'article 27 de cette même loi ;
g) les ressortissants de pays tiers bénéficiant ou bien d'une attestation leur permettant de demeurer sur le territoire luxembourgeois en vertu de l'article 93 de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration ou bien d'un sursis à l'éloignement en vertu de l'article 132 de cette loi ou bien d'une décision de report à l'éloignement en vertu de l'article 125*bis* de cette loi ;
h) les personnes trouvées ou abandonnées sur le territoire de la commune jusqu'à ce que leur situation soit clarifiée ; et
i) les diplomates étrangers et les fonctionnaires de l'Union européenne ou d'une autre institution internationale qui jouissent du statut diplomatique et qui souhaitent être inscrits sur le registre communal, ainsi que les membres de leur famille, tous titulaires d'une carte diplomatique, et les personnes employées par eux auxquels une carte de légitimation est délivrée par le ministre ayant les Affaires étrangères dans ses attributions.[…]

(2) Les personnes visées au paragraphe 1 er, lettre a) sont inscrites sur le registre d'attente.

Ces personnes doivent présenter aux autorités communales compétentes les documents, pièces ou données démontrant que les motifs liés à la sécurité, la salubrité, l'urbanisme ou l'aménagement du territoire ayant justifié leur inscription sur le registre d'attente n'existent plus.

Une inscription sur le registre d'attente ne confère à elle seule aux personnes visées au paragraphe 1er, lettre a) aucun droit ni l'accès aux services communaux.

[…]

Art. 28.

(1) Le bourgmestre ou l'agent délégué inscrit d'office toute personne qui a établi sa résidence habituelle sur le territoire de la commune sans avoir effectué la déclaration d'arrivée prévue par l'article 21. La Police grand-ducale signale au bourgmestre ou à l'agent délégué toute personne se trouvant en infraction avec l'article 21 et dont elle a connaissance.

(2) Si la personne n'a jamais été inscrite auprès d'une commune luxembourgeoise, le bourgmestre ou l'agent délégué l'inscrit d'office sur le registre communal à la date à laquelle sa présence dans la commune a été constatée par une enquête demandée par le bourgmestre ou l'agent délégué et effectuée par la Police grand-ducale.

(3) Si la personne a uniquement omis de faire la déclaration prévue à l'article 21 dans les délais, elle est convoquée par le bourgmestre ou l'agent délégué en vue d'effectuer ladite déclaration dans les huit jours. Lorsque la personne ne donne pas suite à la convocation, le bourgmestre ou l'agent délégué procède à son inscription d'office à l'expiration de ce délai. Cette décision motivée lui est notifiée.

(4) En cas d'inscription d'office, la Police grand-ducale réunit par voie d'enquête les données prévues à l'article 33.

Art. 29.

En cas d'inscription sur le registre communal d'un ressortissant non luxembourgeois ayant eu sa résidence habituelle précédente à l'étranger ou ayant été radié d'office d'un registre communal d'une commune luxembourgeoise, le bourgmestre ou l'agent délégué en informe le ministre ayant l'Immigration respectivement l'Asile dans ses attributions, et le cas échéant la commune du registre de laquelle la personne concernée a été radiée.

Art. 30.

Tout refus définitif d'inscription d'un ressortissant d'un pays tiers sur le registre communal, tout transfert d'inscription d'un ressortissant d'un pays tiers du registre principal sur le registre d'attente et toute radiation d'un ressortissant d'un pays tiers du registre communal sont communiqués par le bourgmestre ou l'agent délégué au ministre ayant respectivement l'Immigration et l'Asile dans ses attributions.

Section 5 – Les radiations du registre communal

Art. 31.

(1) Le bourgmestre ou l'agent délégué procède à la radiation du registre communal :

a) en cas de décès d'une personne y inscrite;
b) en cas de transfert de la résidence habituelle à l'étranger;
c) lorsque la personne concernée ne remplit pas les conditions de résidence de l'article 22;
d) après la notification d'inscription sur le registre communal d'une autre commune luxembourgeoise et à la date de celle-ci, sur base d'une information provenant du Centre dans le cadre de sa mission de gestion du registre national;
e) en cas d'absence du territoire de la commune dépassant six mois sur douze constatée dans le cadre des articles 22 et 25;
f) en cas de non-respect de l'obligation de présentation prévue à l'article 25;
g) après une vérification de la résidence habituelle conformément à l'article 22, paragraphe 2 qui doit avoir lieu après l'expiration de la durée de séjour envisagée, ou au plus tard après trois mois, dans le cas d'un ressortissant de pays tiers ayant fait une déclaration d'arrivée pour un séjour jusqu'à trois mois en application de l'article 36 de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration.
h) […]

Pour toute personne qui établit sa résidence habituelle à l'étranger, la radiation du registre communal a lieu sur la base de la déclaration de départ et à la date de celle-ci. En cas d'absence de déclaration de départ, la radiation a lieu sur base d'une information provenant du Centre dans le cadre de sa mission de gestion du registre national des personnes physiques ou sur base d'une vérification de la résidence habituelle conformément à l'article 22, paragraphe 2.

(2) La radiation du registre principal en faveur d'une inscription sur le registre d'attente intervient :

a) en cas de conflit entre les données inscrites sur le registre principal et celles figurant au registre national ;
b) en cas de décision en faveur d'une inscription sur le registre d'attente prise par le bourgmestre ou l'agent délégué[24] dans le cadre de l'article 22, paragraphe 2 ;
c) en cas de décision de retour telle que visée à l'article 3, lettre h) de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration ou de décision d'éloignement telle que visée à l0article 27 de cette même loi.

(3) La radiation du registre d'attente en faveur d'une inscription sur le registre principal intervient avec effet à la date de l'inscription au registre d'attente :

a) en cas de décision en faveur d'une inscription sur le registre principal prise par le bourgmestre ou l'agent délégué dans le cadre de l'article 22, paragraphe 2;
b) dans le cas prévu à l'article 27, paragraphe 2, alinéa 1 si les personnes concernées ont produit les documents, pièces ou données démontrant que les motifs ayant justifié leur inscription sur le registre d'attente n'existent plus;
c) en cas d'octroi d'une protection internationale aux ressortissants de pays tiers qui ont été titulaires d'une attestation telle que prévue par l'article 7, paragraphe 1er de la loi du 18 décembre 2015 relative à la protection internationale et à la protection temporaire ;

d) en cas d'octroi d'un titre de séjour délivré en vertu de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration aux ressortissants de pays tiers qui ont fait une déclaration d'arrivée pour un séjour de plus de trois mois en application de l'article 40, paragraphe 1er de la loi modifiée du 29 août 2008 précitée.

Art. 32.

Le bourgmestre ou l'agent délégué procède à la radiation d'office du registre communal des personnes qui ont été éloignées du territoire.

Section 6 – Les données inscrites sur le registre communal

Art. 33.

(1) Les données suivantes sont inscrites sur le registre communal :

a) le numéro d'identification;
b) les nom et prénoms;
c) – la résidence habituelle, mentionnant la localité, la rue et le numéro d'immeuble, figurant ou à communiquer au registre national des localités et des rues, prévu par l'article 2, lettre g) de la loi modifiée du 25 juillet 2002 portant réorganisation de l'administration du cadastre et de la topographie, et le code postal ;
   – le cas échéant, le numéro d'ordre établi en exécution de la loi modifiée du 19 mars 1988 sur la publicité foncière en matière de copropriété ;
   – toute précision supplémentaire quant à l'immeuble dans lequel se situe le logement et toute modification intervenue dans la situation de résidence ;
   – l'adresse de résidence de la personne en dehors de la commune où elle a sa résidence habituelle ;
   – le cas échéant, l'adresse de référence prévue par l'article 25 ;
d) les date et lieu de naissance ;
e) la situation de famille ;
f) la ou les nationalités ou le statut d'apatride ;
g) le statut de réfugié ou de protection subsidiaire ;
h) le sexe ;
i) pour les personnes mariées, séparées de corps ou liées par le partenariat en application de la loi modifiée du 9 juillet 2004 relative aux effets légaux de certains partenariats, et pour les personnes veuves, le numéro d'identification pour autant qu'il ait été attribué, les noms, prénoms et dates de naissance des conjoints ou partenaires vivants ou prédécédés ;
j) les numéros d'identification des parents à l'égard desquels la filiation est établie, pour autant que ces numéros aient été attribués ;
k) les numéros d'identification des enfants à l'égard desquels la filiation est établie pour autant que ces numéros aient été attribués ;
l) l'origine et les modifications des données enregistrées ;

m) les date et lieu de décès ;
n) les titres de noblesse des membres de la famille grand-ducale ;
o) l'inscription sur les listes électorales constatant la qualité d'électeur pour les élections législatives, communales ou européennes ; et
p) d'autres données nécessaires pour l'organisation des services de la commune.

(2) Les données prévues au paragraphe 1er, lettres a) à **o)** doivent être identiques aux données prévues aux lettres a) à o) de l'article 5, paragraphe 2.

Les administrations communales transmettent les données qu'elles ont collectées par voie électronique au Centre.

En cas d'impossibilité de transmettre les données par voie électronique, elles sont à transmettre sur support papier.

Le Centre décide de la validation des données transmises par les administrations communales et indique leur qualification prévue par l'article 4, paragraphe 2. Ces données figurent par la suite sur le registre national et le registre communal. Les administrations communales sont responsables de la conformité aux pièces justificatives de toute donnée inscrite ou modifiée et de toute information communiquée au Centre.

(3) Le bourgmestre accorde un droit de consulter les données du registre communal à un ou plusieurs fonctionnaires ou employés communaux de sa commune dans le but d'accomplir les tâches qui leur ont été attribuées. Le bourgmestre s'assure que les données du registre communal soient traitées loyalement et licitement et qu'elles ne soient pas traitées ou conservées de manière incompatible avec les finalités du registre communal.

Art. 34.

Pour chaque information visée à l'article 33, la date à laquelle elle a été inscrite est mentionnée au registre communal.

Sous réserve de l'application de l'article 31, paragraphe 3, toute modification ou rectification d'une information prévue à l'article 33, paragraphe 1er aux lettres a) à n) implique la mention d'une nouvelle date. […]

Le numéro de tout acte d'état civil servant de pièce justificative et le lieu, à savoir la localité et le pays où cet acte a été passé ou transcrit, sont mentionnés au registre communal. Lorsque la pièce justificative est une décision judiciaire ou administrative, l'autorité qui a pris la décision et la date de prise d'effet de la décision sont mentionnées au registre communal.

Les copies numériques ou les photocopies des pièces justificatives des données inscrites sur le registre communal doivent être conservées par les communes.

Un règlement grand-ducal peut fixer les modalités et critères en vertu desquels les pièces justificatives doivent être conservées.

Chapitre 3 – La protection des données inscrites sur les registres

Art. 35.

Toute personne, dont les données font l'objet d'une inscription sur le registre national ou communal, a le droit de consulter et d'obtenir communication des données qui la concernent suivant les modalités fixées ci-dessous.

Art. 36.

(1) Toute demande de communication de données doit être adressée soit directement au guichet de la commune sur base d'un formulaire, soit par lettre simple ou par voie électronique au ministre pour les données inscrites sur le registre national ou au bourgmestre pour les données inscrites sur le registre communal. Elle doit être datée et signée. Une demande introduite par voie électronique doit soit comporter une signature électronique avancée sur base d'un certificat qualifié, soit être soumise grâce à un dispositif informatique qui garantit l'identité du demandeur et l'authenticité de la demande.

La demande de communication est présentée par la personne concernée, son tuteur, son curateur, son administrateur légal, son administrateur ad hoc ou son mandataire spécial. Si la personne concernée est mineure d'âge non émancipée, la demande doit être faite par un des parents qui exerce l'autorité parentale ou par le tuteur. La demande doit être accompagnée d'une photocopie de la pièce d'identité de l'auteur de la demande et, le cas échéant, du titre en vertu duquel il agit.

Les données sont soit communiquées, selon le souhait de l'auteur de la demande, par lettre ou par courrier électronique, soit imprimées au guichet et ce à chaque fois sous forme d'un extrait du registre national reproduisant de manière exacte l'ensemble des données relatives à la personne concernée. Cet extrait est établi en langues française, allemande et luxembourgeoise.

(2) La demande est refusée si elle est introduite par une personne qui ne remplit pas les conditions et les formalités requises par la présente loi. Tout refus de communication des données est motivé et le demandeur en est informé par la voie appropriée, selon les modalités prescrites au paragraphe 1er.

(3) Il est mentionné sur l'extrait remis au demandeur que les informations qu'il contient reproduisent de manière exacte l'ensemble des données de cette personne inscrites sur le registre visé et que cet extrait ne vaut pas extrait d'état civil.

Art. 37.

(1) Si les données communiquées à une personne en vertu de l'article 36 se révèlent être incomplètes ou inexactes, la personne concernée peut en demander la rectification.

Toute demande de rectification de données doit être adressée soit directement au guichet de la commune sur base d'un formulaire, soit par lettre simple ou par voie électronique au ministre pour

les données inscrites sur le registre national ou au bourgmestre pour les données inscrites sur le registre communal. Elle doit être datée et signée. Une demande introduite par voie électronique doit soit comporter une signature électronique avancée sur base d'un certificat qualifié, soit être soumise grâce à un dispositif informatique qui garantit l'identité du demandeur et l'authenticité de la demande.

La demande de rectification est présentée par la personne concernée, son tuteur, son curateur, son administrateur légal, son administrateur ad hoc ou son mandataire spécial. Si la personne concernée est mineure d'âge non émancipée, la demande doit être faite par un des parents qui exerce l'autorité parentale ou par le tuteur. La demande doit être accompagnée d'une photocopie de la pièce d'identité de l'auteur de la demande et, le cas échéant, du titre en vertu duquel il agit. Toute demande de rectification doit être motivée.

La personne exerçant son droit de rectification fournit à l'appui de sa requête tous les éléments de preuve. A sa demande, la personne concernée est entendue par le ministre ou le bourgmestre et peut se faire assister par une personne de son choix.

Tout refus de rectification est motivé et notifié par lettre recommandée à l'auteur de la demande.

(2) A l'issue de la procédure de rectification, la personne concernée, son tuteur, son curateur, son administrateur légal, son administrateur ad hoc ou son mandataire spécial reçoit un extrait rectifié du registre national, respectivement du registre communal. Cet extrait est établi en langues française, allemande et luxembourgeoise.

Art. 38.

Toute personne, dont les données font l'objet d'une inscription sur le registre national, a le droit d'obtenir la liste des autorités, administrations, services, institutions ou organismes qui ont, au cours des six mois précédant sa demande, consulté ou mis à jour ses données au registre national ou qui en ont reçu communication, sauf si une consultation ou une communication a été faite par ou à une autorité chargée de la sécurité de l'Etat, de la défense, de la sécurité publique, de l'établissement ou du recouvrement des taxes, impôts et droits perçus par ou pour le compte de l'Etat, de la prévention, de la recherche, de la constatation et de la poursuite d'infractions pénales, y compris de la lutte contre le blanchiment d'argent, ou du déroulement d'autres procédures judiciaires. La procédure prévue à l'article 36 s'applique.

Art. 39.

Tout ayant droit des personnes visées à l'article 35 peut obtenir un extrait du registre national ou un certificat établi sur base de ce registre, pour autant que les informations qu'il contient se réfèrent directement à sa personne.

La demande est formulée par l'ayant droit concerné, son tuteur, son curateur, son administrateur légal, son administrateur ad hoc ou son mandataire spécial. Les mineurs d'âge non émancipés sont

représentés par celui de leurs parents qui exerce l'autorité parentale ou par le tuteur. La procédure prévue à l'article 36 s'applique.

Art. 40.

Tout extrait et tout certificat remis au demandeur dans le cadre des articles 36 à 39 sont signés par le directeur ou par un agent délégué du Centre, s'ils concernent le registre national, ou par le bourgmestre ou l'agent délégué, s'ils concernent le registre communal.

Art. 41.

Les données ou listes de données figurant au registre national ou communal ne peuvent être communiquées à des tiers. Cette interdiction ne vise pas les autorités, administrations, services, institutions ou organismes habilités, par ou en vertu de la loi, à obtenir de telles données ou listes de données et ce pour les informations sur lesquelles porte cette habilitation.

Art. 42.

Sur demande écrite et signée mentionnant le but poursuivi et l'utilisation projetée, le ministre peut autoriser la délivrance à des tiers de données statistiques tirées du registre national à condition que celles-ci ne permettent pas l'identification des personnes inscrites sur le registre national.

Le ministre garantit la non-divulgation de données à caractère confidentiel lors de la délivrance de statistiques. Les données utilisées pour la production de statistiques sont considérées comme confidentielles lorsqu'elles permettent l'identification, directe ou indirecte, d'une personne physique ou comportent un risque de divulgation d'informations individuelles. Pour déterminer si une personne physique est identifiable, il est tenu compte de tous les moyens dont on pourrait raisonnablement admettre qu'ils puissent être utilisés par un tiers pour identifier ladite personne.

Chapitre 4 – Dispositions pénales

Art. 43.

Toute absence de déclaration prévue à l'article 21, paragraphe 1er, ainsi que toute déclaration faite après l'expiration des délais prévus à l'article 21, paragraphe 2, est punie d'une amende de 25 à 250 euros.

Chapitre 5 – Dispositions modificatives, abrogatoires, transitoires et finales

Section 1 – Dispositions modificatives

Art. 44.

L'article 104 du Code civil est modifié comme suit :

«Art. 104. La preuve de l'intention résultera d'une déclaration expresse faite à la commune où on aura transféré son domicile.»

Art. 45.

La loi modifiée du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales ne s'applique plus aux personnes physiques.

Art. 46.

Toute référence à «la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales » et qui vise les personnes physiques s'entend comme référence à «la loi du 19 juin 2013 relative à l'identification des personnes physiques ».

Toute référence au « répertoire général » et qui vise les personnes physiques s'entend comme référence au « registre national des personnes physiques ».

Toute référence au « matricule » ou au « numéro d'identité » s'entend comme référence au « numéro d'identification ».

Toute référence aux « registres de la population » s'entend comme référence aux « registres communaux des personnes physiques ».

Art. 47.

L'article 76, alinéa 1er de la loi communale modifiée du 13 décembre 1988 est modifié comme suit :

a) Le point 1° est supprimé.

b) Le point 2° est remplacé par un nouveau point 2° ayant la teneur suivante :

«2° la délivrance d'extraits du registre communal des personnes physiques et de certificats établis en tout ou en partie d'après ce registre ;».

Art. 48.

La deuxième phrase de l'article 10, deuxième alinéa, de la loi électorale modifiée du 18 février 2003 est supprimée.

Section 2 – Dispositions abrogatoires

Art. 49.

L'arrêté grand-ducal du 30 août 1939 portant introduction de la carte d'identité obligatoire est abrogé.

Art. 50.

La loi modifiée du 22 décembre 1886 concernant le recensement de population à faire en exécution de la loi électorale est abrogée.

Section 3 – Dispositions transitoires

Art. 51.

(1) Chaque personne peut acter l'exactitude des données la concernant, qui ont été reprises au registre national des personnes physiques le 1 er juillet 2013, en contresignant un extrait de données et en le retournant à un agent de l'administration communale ou du Centre.

Le cas échéant, cet extrait peut s'accompagner d'une demande de rectification de données, datée et signée par la personne concernée, son représentant légal ou son mandataire spécial.

Les mineurs d'âge non émancipés sont représentés par celui de leurs parents qui exerce l'autorité parentale ou par le tuteur. Le représentant doit joindre une photocopie de la pièce d'identité et du titre en vertu duquel il agit.

Toute demande de rectification doit être motivée. La personne exerçant son droit de rectification fournit à l'appui de sa requête tous les éléments de preuve méritant d'être pris en considération. Tout refus de rectification est motivé et notifié par lettre simple au demandeur.

(2) En ce qui concerne les ressortissants de pays tiers qui sont titulaires d'une attestation en cours de validité telle que prévue par les articles 6, paragraphe 5 ou 62 de la loi modifiée du 5 mai 2006 relative au droit d'asile et à des formes complémentaires de protection et qui avant l'entrée en vigueur de la présente loi ont été inscrits sur un registre de la population, les bourgmestres ou les agents[33] délégués des communes sur le territoire desquelles ces personnes ont établi leur résidence habituelle effectuent un transfert des données de ces personnes du registre de la population en vigueur avant la présente loi au registre d'attente institué par la présente loi.

(3) Les données concernant l'historique des personnes inscrites sur les registres de la population des communes sont reprises dans les registres communaux des personnes physiques.

Art. 52.

Les cartes d'identité délivrées en application de l'arrêté grand-ducal précité du 30 août 1939 restent valables jusqu'à leur date d'expiration.

Art. 52*bis*

Jusqu'au 1er janvier 2016, la référence au « registre communal des personnes physiques » figurant à l'article 1er, paragraphe 1er, lettre a) s'entend comme référence au « registre de la population ».

Section 4 – Disposition finale

Art. 53.

La référence à la présente loi peut se faire sous une forme abrégée en recourant à l'intitulé suivant :

« loi du 19 juin 2013 relative à l'identification des personnes physiques ».

Section 5 – Entrée en vigueur

Art. 54.

Les dispositions figurant au chapitre 1er, sections 3 et 4, entrent en vigueur le 1er jour du mois après la publication de la loi au Mémorial.

Les dispositions figurant aux articles 1er à 3, aux articles 12 à 16, à l'article 45, à l'article 46 alinéas 1 à 3, à l'article 47 lettre a), ainsi que celles figurant aux articles 49, 52, 52bis et 53 entrent en vigueur le 1er juillet 2014.

Les dispositions figurant aux articles 35 à 42 pour autant qu'elles concernent le registre national des personnes physiques entrent en vigueur le 1er juillet 2014.

Les autres dispositions entrent en vigueur le 1er janvier 2016.

Mandons et ordonnons que la présente loi soit insérée au Mémorial pour être exécutée et observée par tous ceux que la chose concerne.

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Digitalisation

FICHE FINANCIÈRE

Les amendements gouvernementaux n'ont pas d'impact financier.

*

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

CHECK DURABILITÉ - NOHALTEGKEETSCHECK

La présente page interactive nécessite au minimum la version 8.1.3 d'Adobe Acrobat® Reader®. La dernière version d'Adobe Acrobat Reader pour tous systèmes (Windows®, Mac, etc.) est téléchargeable gratuitement sur le site de Adobe Systems Incorporated.

Ministre responsable :	La Ministre à la Digitalisation
Projet de loi ou amendement :	Amendement du Projet de loi relatif à la mise en place du portefeuille européen d'identité numérique et portant mise en œuvre du règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique et modifiant la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques

Le check durabilité est un outil d'évaluation des actes législatifs par rapport à leur impact sur le developpement durable. Son objectif est de donner l'occasion d'introduire des aspects relatifs au développement durable à un stade préparatoire des projets de loi. Tout en faisant avancer ce thème transversal qu'est le developpement durable, il permet aussi d'assurer une plus grande cohérence politique et une meilleure qualité des textes législatifs.

1. Est-ce que le projet de loi sous rubrique a un impact sur le champ d'action (1-10) du 3ème Plan national pour un Développement durable ?
2. En cas de réponse négative, expliquez-en succinctement les raisons.
3. En cas de réponse positive sous 1., quels seront les effets positifs et / ou négatifs éventuels de cet impact?
4. Quelles catégories de personnes seront touchées par cet impact ?
5. Quelles mesures sont envisagées afin de pouvoir atténuer les effets négatifs et comment pourront être renforcés les aspects positifs de cet impact ?

Afin de faciliter cet exercice, l'instrument du contrôle de la durabilité est accompagné par des points d'orientation – **auxquels il n'est pas besoin de réagir ou répondre mais qui servent uniquement d'orientation**
- , ainsi que par une documentation sur les dix champs d'actions précités.

1. Assurer une inclusion sociale et une éducation pour tous.

Poins d'orientation
Documentation

☒ Oui ☐ Non

L'introduction du portefeuille peut, de par la convivialité et l'accessibilité exigées par le règlement européen qui le met en place, contribuer à augmenter l'inclusion sociale dans le domaine de démarches administratives.

2. Assurer les conditions d'une population en bonne santé.

Poins d'orientation
Documentation

☐ Oui ☒ Non

Ce projet de loi a pour objet la mise en place du portefeuille européen d'identité numérique et n'a donc pas de lien avec la santé de la population.

3. Promouvoir une consommation et une production durables.

Poins d'orientation Documentation ☐ Oui ☒ Non

Ce projet de loi concerne la mise en place du portefeuille européen d'identité numérique et n'a pas d'impact sur la consommation ou la production durables.

4. Diversifier et assurer une économie inclusive et porteuse d'avenir.

Poins d'orientation Documentation ☒ Oui ☐ Non

Le portefeuille, s'inscrivant dans les efforts de digitalisation de l'État, permet des économies substantielles par rapport aux démarches basées sur le papier.

5. Planifier et coordonner l'utilisation du territoire.

Poins d'orientation Documentation ☐ Oui ☒ Non

Ce projet de loi, relatif à la mise en place du portefeuille européen d'identité numérique, n'a pas d'impact sur la coordination et la planification de l'utilisation du territoire luxembourgeois.

6. Assurer une mobilité durable.

Poins d'orientation Documentation ☐ Oui ☒ Non

Ce projet de loi n'a pas d'impact sur la mobilité durable.

7. Arrêter la dégradation de notre environnement et respecter les capacités des ressources naturelles.

Poins d'orientation Documentation ☐ Oui ☒ Non

Ce projet de loi n'a pas d'effet sur l'environnement ou les ressources naturelles.

8. Protéger le climat, s'adapter au changement climatique et assurer une énergie durable.

Poins d'orientation Documentation ☐ Oui ☒ Non

Ce projet de loi n'a pas d'impact direct sur le climat, le changement climatique ou l'énergie durable.

9. Contribuer, sur le plan global, à l'éradication de la pauvreté et à la cohérence des politiques pour le développement durable.

Poins d'orientation Documentation ☐ Oui ☒ Non

Ce projet de loi n'a pas d'impact sur la pauvreté ou sur la cohérence des politiques pour le développement durable.

10. Garantir des finances durables.

Poins d'orientation Documentation ☐ Oui ☒ Non

Ce projet de loi ne contribuera pas financièrement à l'action climatique, ni au développement durable.

Cette partie du formulaire est facultative - Veuillez cocher la case correspondante

En outre, et dans une optique d'enrichir davantage l'analyse apportée par le contrôle de la durabilité, il est proposé de recourir, de manière facultative, à une évaluation de l'impact des mesures sur base d'indicateurs retenus dans le PNDD. Ces indicateurs sont suivis par le STATEC.

Continuer avec l'évaluation ? ☐ Oui ☒ Non

(1) Dans le tableau, choisissez l'évaluation : **non applicable**, ou de 1 = **pas du tout probable** à 5 = **très possible**

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
1		Contribue à la réduction du taux de risque de pauvreté ou d'exclusion sociale	Taux de risque de pauvreté ou d'exclusion sociale	% de la population
1		Contribue à la réduction du nombre de personnes vivant dans des ménages à très faible intensité de travail	Personnes vivant dans des ménages à très faible intensité de travail	milliers
1		Contribue à la réduction de la différence entre taux de risque de pauvreté avant et après transferts sociaux	Différence entre taux de risque de pauvreté avant et après transferts sociaux	pp
1		Contribue à l'augmentation du taux de certification nationale	Taux de certification nationale	%
1		Contribue à l'apprentissage tout au long de la vie en % de la population de 25 à 64 ans	Apprentissage tout au long de la vie en % de la population de 25 à 64 ans	%
1		Contribue à l'augmentation de la représentation du sexe sous-représenté dans les organes de prises de décision	Représentation du sexe sous-représenté dans les organes de prises de décision	%
1		Contribue à l'augmentation de la proportion des sièges détenus par les femmes au sein du parlement national	Proportion des sièges détenus par les femmes au sein du parlement national	%
1		Contribue à l'amélioration de la répartition des charges de travail domestique dans le sens d'une égalité des genres	Temps consacré au travail domestique non payé et activités bénévoles	hh:mm
1		Contribue à suivre l'impact du coût du logement afin de circonscrire le risque d'exclusion sociale	Indice des prix réels du logement	Indice 2015=100
2		Contribue à la réduction du taux de personnes en surpoids ou obèses	Taux de personnes en surpoids ou obèses	% de la population
2		Contribue à la réduction du nombre de nouveaux cas d'infection au HIV	Nombre de nouveaux cas d'infection au HIV	Nb de personnes
2		Contribue à la réduction de l'incidence de l'hépatite B pour 100 000 habitants	Incidence de l'hépatite B pour 100 000 habitants	Nb de cas pour 100 000 habitants

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
2		Contribue à la réduction du nombre de décès prématurés liés aux maladies chroniques pour 100 000 habitants	Nombre de décès prématurés liés aux maladies chroniques pour 100 000 habitants	Nb de décès pour 100 000 habitants
2		Contribue à la réduction du nombre de suicides pour 100 000 habitants	Nombre de suicides pour 100 000 habitant	Nb de suicides pour 100 000 habitants
2		Contribue à la réduction du nombre de décès liés à la consommation de psychotropes	Nombre de décès liés à la consommation de psychotropes	Nb de décès
2		Contribue à la réduction du taux de mortalité lié aux accidents de la route pour 100 000 habitants	Taux de mortalité lié aux accidents de la route pour 100 000 habitants	Nb de décès pour 100 000 habitants
2		Contribue à la réduction de la proportion de fumeurs	Proportion de fumeurs	% de la population
2		Contribue à la réduction du taux de natalité chez les adolescentes pour 1 000 adolescentes	Taux de natalité chez les adolescentes pour 1 000 adolescentes	Nb de naissance pour 1000 adolescentes
2		Contribue à la réduction du nombre d'accidents du travail	Nombre d'accidents du travail (non mortel + mortel)	Nb d'accidents
3		Contribue à l'augmentation de la part de la surface agricole utile en agriculture biologique	Part de la surface agricole utile en agriculture biologique	% de la SAU
3		Contribue à l'augmentation de la productivité de l'agriculture par heure travaillée	Productivité de l'agriculture par heure travaillée	Indice 2010=100
3		Contribue à la réduction d'exposition de la population urbaine à la pollution de l'air par les particules fines	Exposition de la population urbaine à la pollution de l'air par les particules fines	Microgrammes par m^3
3		Contribue à la réduction de production de déchets par habitant	Production de déchets par habitant	kg/hab
3		Contribue à l'augmentation du taux de recyclage des déchets municipaux	Taux de recyclage des déchets municipaux	%
3		Contribue à l'augmentation du taux de recyclage des déchets d'équipements électriques et électroniques	Taux de recyclage des déchets d'équipements électriques et électroniques	%
3		Contribue à la réduction de la production de déchets dangereux	Production de déchets dangereux	tonnes
3		Contribue à l'augmentation de la production de biens et services environnementaux	Production de biens et services environnementaux	millions EUR
3		Contribue à l'augmentation de l'intensité de la consommation intérieure de matière	Intensité de la consommation intérieure de matière	tonnes / millions EUR
4		Contribue à la réduction des jeunes sans emploi et ne participant ni à l'éducation ni à la formation (NEET)	Jeunes sans emploi et ne participant ni à l'éducation ni à la formation (NEET)	% de jeunes

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
4		Contribue à l'augmentation du pourcentage des intentions entreprenariales	Pourcentage des intentions entreprenariales	%
4		Contribue à la réduction des écarts de salaires hommes-femmes	Ecarts de salaires hommes-femmes	%
4		Contribue à l'augmentation du taux d'emploi	Taux d'emploi	% de la population
4		Contribue à la création d'emplois stables	Proportion de salariés ayant des contrats temporaires	% de l'emploi total
4		Contribue à la réduction de l'emploi à temps partiel involontaire	Emploi à temps partiel involontaire	% de l'emploi total
4		Contribue à la réduction des salariés ayant de longues heures involontaires	Salariés ayant de longues heures involontaires	% de l'emploi total
4		Contribue à la réduction du taux de chomage	Taux de chomage	% de la population active
4		Contribue à la réduction du taux de chomage longue durée	Taux de chomage longue durée	% de la population active
4		Contribue à l'augmentation du taux de croissance du PIB réel (moyenne sur 3 ans)	Taux de croissance du PIB réel (moyenne sur 3 ans)	%
4		Contribue à l'augmentation de la productivité globale des facteurs	Productivité globale des facteurs	Indice 2010=100
4		Contribue à l'augmentation de la productivité réelle du travail par heures travaillées (taux de croissance moyen sur 3 ans)	Productivité réelle du travail par heures travaillées (taux de croissance moyen sur 3 ans)	%
4		Contribue à l'augmentation de la productivité des ressources	Productivité des ressources	Indice 2000=100
4		Contribue à l'augmentation de la valeur ajoutée dans l'industrie manufacturière	Valeur ajoutée dans l'industrie manufacturière, en proportion de la valeur ajoutée totale des branches	% de la VA totale
4		Contribue à l'augmentation de l'emploi dans l'industrie manufacturière	Emploi dans l'industrie manufacturière, en proportion de l'emploi total	% de l'emploi
4		Contribue à la réduction des émissions de CO2 de l'industrie manufacturière	Émissions de CO2 de l'industrie manufacturière par unité de valeur ajoutée	% de la VA totale
4		Contribue à l'augmentation des dépenses intérieures brutes de R&D	Niveau des dépenses intérieures brute de R&D	% du PIB
4		Contribue à l'augmentation du nombre de chercheurs	Nombre de chercheurs pour 1000 actifs	nb pour 1000 actifs

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
5		Contribue à la réduction du nombre de personnes confrontées à la délinquance, à la violence ou au vandalisme dans leur quartier, en proportion de la population totale	Nombre de personnes confrontées à la délinquance, à la violence ou au vandalisme dans leur quartier, en proportion de la population totale	%
5		Contribue à la réduction du pourcentage du territoire transformé en zones artificialisées	Zones artificialisées	% du territoire
5		Contribue à l'augmentation des dépenses totales de protection environnementale	Dépenses totales de protection environnementale	millions EUR
6		Contribue à l'augmentation de l'utilisation des transports publics	Utilisation des transports publics	% des voyageurs
7		Contribue à la fertilité des sols sans nuire à la qualité des eaux de surface et/ou les eaux souterraines, de provoquer l'eutrophisation des eaux et de dégrader les écosystèmes terrestres et/ou aquatiques (unité: kg d'azote par ha SAU)?	Bilan des substances nutritives d'azote	kg d'azote par ha SAU
7		Contribue à la fertilité des sols sans nuire à la qualité des eaux de surface et/ou les eaux souterraines, de provoquer l'eutrophisation des eaux et de dégrader les écosystèmes terrestres et/ou aquatiques (unité: kg de phosphore par ha SAU)	Bilan des substances nutritives phosphorées	kg de phosphore par ha SAU
7		Contribue à une consommation durable d'une eau de robinet de qualité potable	Part des dépenses en eau dans le total des dépenses des ménages	%
7		Contribue à l'augmentation du pourcentage des masses d'eau de surface naturelles ayant atteint un état écologique "satisfaisant" et des masses d'eau souterraine ayant atteint un bon état chimique	Pourcentage des masses d'eau de surface naturelles ayant atteint un état écologique "satisfaisant" et des masses d'eau souterraine ayant atteint un bon état chimique	%
7		Contribue à l'augmentation de l'efficacité de l'usage de l'eau	Efficacité de l'usage de l'eau	m3/millions EUR
7		Contribuer à une protection des masses d'eau de surfaces et les masses d'eau souterraine par des prélèvements durables et une utilisation plus efficiente de l'eau	Indice de stress hydriques	%
7		Contribue à la préservation et/ou l'augmentation de la part de zones agricoles et forestières	Part des zones agricoles et forestières	% du territoire
7		Contribue à l'augmentation de la part du territoire designée comme zone protégée pour la biodiversité	Part du territoire désignée comme zone protégée pour la biodiversité	% du territoire
7		Contribue à la protection des oiseaux inscrits sur la liste rouge des espèces menacées	Nombre d'espèces sur la liste rouge des oiseaux	Nb d'espèces
7		Contribue à la lutte contre les espèces exotiques invasives inscrites sur la liste noire	Nombre de taxons sur la liste noire des plantes vasculaires	Nb de taxons
7		Contribue à la favorabilité de l'état de conservation des habitats	Etat de conservation des habitats	% favorables

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
8		Contribue à la réduction de l'intensité énergétique	Intensité énergétique	TJ/millions EUR
8		Contribue à la réduction de la consommation finale d'énergie	Consommation finale d'énergie	GWh
8		Contribue à l'augmentation de la part des énergies renouvelables dans la consommation finale d'énergie	Part des énergies renouvelables dans la consommation finale d'énergie	%
8		Contribue à la réduction de la part des dépenses énergétiques dans le total des dépenses des ménages	Part des dépenses énergétiques dans le total des dépenses des ménages	%
8		Contribue à la réduction du total des émissions de gaz à effet de serre	Total des émissions de gaz à effet de serre	millions tonnes CO2
8		Contribue à la réduction des émissions de gaz à effet de serre hors SEGE	Emissions de gaz à effet de serre hors SEGE	millions tonnes CO2
8		Contribue à la réduction de l'intensité des émissions de gaz à effet de serre	Intensité des émissions de gaz à effet de serre	kg CO2 / EUR
9		Contribue à l'augmentation de l'aide au développement - Education	Aide au développement - Education	millions EUR
9		Contribue à l'augmentation de l'aide au développement - Agriculture	Aide au développement - Agriculture	millions EUR (prix constant 2016)
9		Contribue à l'augmentation de l'aide au développement - Santé de base	Aide au développement - Santé de base	millions EUR (prix constant 2016)
9		Contribue à l'augmentation de la part des étudiants des pays en développement qui étudient au Luxembourg	Part des étudiants des pays en développement qui étudient au Luxembourg	%
9		Contribue à l'augmentation du montant des bourses d'étude	Montant des bourses d'étude	millions EUR
9		Contribue à l'augmentation de l'aide au développement - Eau et assainissement	Aide au développement - Eau et assainissement	millions EUR (prix constant 2016)
9		Contribue à l'augmentation de l'aide au développement - Energie	Aide au développement - Energie	millions EUR (prix constant 2016)
9		Contribue à l'augmentation de l'aide au développement - Lois et règlements commerciaux	Aide au développement - Lois et règlements commerciaux	millions EUR (prix constant 2016)
9		Contribue à l'augmentation du montant des dépenses sociales expimé en ratio du PIB	Montant des dépenses sociales exprimé en ratio du PIB	% du PIB
9		Contribue à l'augmentation de l'aide publique nette au développement, montant alloué aux pays les moins avancés (absolu)	Aide publique nette au développement, montant alloué aux pays les moins avancés	millions EUR (prix constant 2016)

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
9		Contribue à l'augmentation de l'aide publique nette au développement, montant alloué aux pays les moins avancés (en proportion du montant total d'aide au développement)	Aide publique nette au développement, montant alloué aux pays les moins avancés, en proportion du montant total d'aide au développement	%
9		Contribue à l'augmentation de l'aide au développement - Prévention et préparation aux catastrophes	Aide au développement - Prévention et préparation aux catastrophes	millions EUR (prix constant 2016)
9		Contribue à l'engagement international de 100 Mrds USD pour dépenses reliées au climat	Contribution à l'engagement international de 100 Mrds USD pour dépenses reliées au climat	millions EUR
9		Contribue à l'augmentation de l'aide au développement avec marqueur biodiversité	Aide au développement avec marqueur biodiversité	millions EUR (prix constant 2016)
9		Contribue à l'augmentation de l'aide publique nette au développement, montant total, en proportion du revenu national brut	Aide publique nette au développement, montant total, en proportion du revenu national brut	% du RNB
9		Contribue à l'augmentation de l'aide au développement - coopération technique	Aide au développement – coopération technique	millions EUR (prix constant 2016)
9		Contribue à la réduction de la dette publique en proportion du Produit Intérieur Brut	Dette publique en proportion du Produit Intérieur Brut	% du Pib
9		Contribue à l'augmentation du montant investi dans des projets de soutien à l'enseignement supérieur	Montant investi dans des projets de soutien à l'enseignement supérieur	millions EUR (prix constant 2016)
9		Contribue à l'augmentation de l'aide publique au développement - renforcement de la société civile dans les pays partenaires	Aide publique au développement - renforcement de la société civile dans les pays partenaires	millions EUR (prix constant 2016)
10		Contribue à l'action climatique dans les pays en développement et à la protection du climat au niveau global	Contribution des CDM à la réduction des émissions de gaz à effet de serre	millions EUR
10		Contribue à l'augmentation de l'alimentation du fonds climat énergie	Fonds climat énergie	millions EUR
10		Contribue à l'augmentation de la part des taxes environnementales dans le total des taxes nationales	Part des taxes environnementales dans le total des taxes nationales	% du revenu fiscal

Afin d'enregistrer une version verrouillée du formulaire, merci de le signer digitalement en cliquant ici :

Digitally signed by:
Gaston Schmit
Ministry for Digitalisation
Date: 13/10/2026 15:45:20

ME_SGCG_CD_F_202204_4

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

FICHE D'ÉVALUATION D'IMPACT
MESURES LÉGISLATIVES, RÉGLEMENTAIRES ET AUTRES

La présente page interactive nécessite au minimum la version 8.1.3 d'Adobe Acrobat® Reader®. La dernière version d'Adobe Acrobat Reader pour tous systèmes (Windows®, Mac, etc.) est téléchargeable gratuitement sur le site de Adobe Systems Incorporated.

1. Coordonnées du projet

Intitulé du projet :	Amendement du projet de loi relatif à la mise en place du portefeuille européen d'identité numérique et portant mise en oeuvre du règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique et modifiant la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques
Ministre initiateur :	La Ministre de la Digitalisation
Auteur(s) :	France Oly
Téléphone :	247-72127
Courriel :	france.oly@digital.etat.lu
Objectif du projet :	Les présents amendements du projet de loi 8583 se proposent de mettre en oeuvre une partie du règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 et des règlements d'exécutiony relatifs en ce qui concerne l'établissement du cadre européen relatif à une identité numérique. Il y a lieu de noter que le texte proposé concerne les dispositions du règlement (UE) 2024/1183 relatives au développement et à la fourniture de l'outil d'un portefeuille numérique.
Autre(s) Ministère(s) / Organisme(s) / Commune(s) impliqué(e)(s) :	Institut Luxembourgeois de Régulation
Date :	13/10/2026

2. Objectifs à valeur constitutionnelle

Le projet contribue-t-il à la réalisation des objectifs à valeur constitutionnelle ? ☒ Oui ☐ Non

Dans l'affirmative, veuillez sélectionner les objectifs concernés et veuillez fournir une brève explication dans la case «Remarques» indiquant en quoi cet ou ces objectifs sont réalisés :

- ☐ Garantir le droit au travail et veiller à assurer l'exercice de ce droit
- ☐ Promouvoir le dialogue social
- ☐ Veiller à ce que toute personne puisse vivre dignement et dispose d'un logement approprié
- ☐ Garantir la protection de l'environnement humain et naturel en œuvrant à l'établissement d'un équilibre durable entre la conservation de la nature, en particulier sa capacité de renouvellement, ainsi que la sauvegarde de la biodiversité, et satisfaction des besoins des générations présentes et futures
- ☐ S'engager à lutter contre le dérèglement climatique et œuvrer en faveur de la neutralité climatique
- ☐ Protéger le bien-être des animaux
- ☐ Garantir l'accès à la culture et le droit à l'épanouissement culturel

☐ Promouvoir la protection du patrimoine culturel

☐ Promouvoir la liberté de la recherche scientifique dans le respect des valeurs d'une société démocratique fondée sur les droits fondamentaux et les libertés publiques

Remarques : valeur constitutionnelle: Protection des données
Le portefeuille permettra à l'utilisateur de choisir quelles données d'identité personnelle il veut partager ("cherrypicking") au lieu de par exemple montrer par le biais de la la carte d'identité l'integralité des informations y réunies.

3. Mieux légiférer

1) Chambre(s) professionnelle(s) à saisir / saisi(e)s pour avis [1] :

☒ Chambre des fonctionnaires et employés publics
☒ Chambre des salariés
☒ Chambre des métiers
☒ Chambre de commerce
☒ Chambre d'agriculture

[1] Veuillez indiquer la/les Chambre(s) professionnelle(s) saisie(s) du projet sous rubrique suite à son approbation par le Conseil de gouvernement.

2) Autre(s) partie(s) prenante(s) (organismes divers, citoyens, ...) à saisir / saisi(e)s pour avis : ☒ Oui ☐ Non

Si oui, laquelle / lesquelles : CNPD

Remarques / Observations :

3) En cas de transposition de directives européennes, le principe « la directive, rien que la directive » est-il respecté ? ☐ Oui ☐ Non ☒ N.a. [2]

Si non, pourquoi ?

4) Destinataires du projet :

- Entreprises / Professions libérales : ☒ Oui ☐ Non
- Citoyens : ☒ Oui ☐ Non
- Administrations : ☒ Oui ☐ Non

5) Le principe « Think small first » est-il respecté ? ☐ Oui ☐ Non ☒ N.a. [2]
(c.-à-d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité ?)

Remarques / Observations :

6) Le projet contribue-t-il à la simplification administrative, notamment en supprimant ou en simplifiant des régimes d'autorisation et de déclaration existants, en réduisant les délais de réponse de l'administration, en réduisant la charge administrative pour les destinataires ou en améliorant la qualité des procédures ou de la règlementation ? ☒ Oui ☐ Non

Remarques / Observations :	Le portefeuille d'identité numérique simplifie les procédures d'identification et d'authentification en ligne, en rendant superflue la création d'un compte utilisateur, et, en particulier, il offre un niveau de sécurité accru sur la signature

7) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel ? ☒ Oui ☐ Non ☐ N.a. [2]

Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?	Le projet émet les règles d'utilisation des données à caractère personnel pour le CTIE en tant que fournisseur des données d'identification personnelle, et pour le CGSD en tant que bureau d'enregistrement des parties utilisatrices du portefeuille. Et dans la vision d'ajouter des "attributs" au portefeuille: Il s'agit de toute donnée pour laquelle un justificatif électronique peut être produite.

8) Y a-t-il un besoin en formation du personnel de l'administration concernée ? ☐ Oui ☐ Non ☒ N.a. [2]

Si oui, lequel ?	
Remarques / Observations :	

[2] N.a. : non applicable.

4. Digitalisation et données

9) Y a-t-il une nécessité d'adapter un système informatique auprès de l'État (e-Government ou application back-office) ☒ Oui ☐ Non

Si oui, quel est le délai pour disposer du nouveau système ?	environ 2 mois

10) Le projet tient-il compte du principe « digital by default » (priorisation de la voie numérique) ? ☒ Oui ☐ Non

11) Le projet crée-t-il une démarche administrative qui nécessite des informations ou des données à caractère personnel sur les administrés ? ☒ Oui ☐ Non

Si oui, ces informations ou données à caractère personnel peuvent-elles être obtenues auprès d'une ou plusieurs administrations conformément au principe «Once only» ?	oui.

12) Le projet envisage-t-il la création ou l'adaptation d'une banque de données ? ☒ Oui ☐ Non

5. Égalité des chances (à remplir pour les projets de règlements grand-ducaux) [3]

13) Le projet est-il :

- principalement centré sur l'égalité des femmes et des hommes ? ☐ Oui ☒ Non
- positif en matière d'égalité des femmes et des hommes ? ☐ Oui ☒ Non

Si oui, expliquez de quelle manière :

- neutre en matière d'égalité des femmes et des hommes ? ☒ Oui ☐ Non

Si oui, expliquez pourquoi : Il n'y a aucune distinction entre un utilisateur féminin ou masculin du portefeuille d'identité numérique

- négatif en matière d'égalité des femmes et des hommes ? ☐ Oui ☒ Non

Si oui, expliquez de quelle manière :

14) Y a-t-il un impact financier différent sur les femmes et les hommes ? ☐ Oui ☒ Non ☐ N.a. [2]

Si oui, expliquez de quelle manière :

[3] Pour les projets de loi, il convient de se référer au point 1 « Assurer une inclusion sociale et une éducation pour tous. » du Nohaltegkeetscheck.

6. Projets nécessitant une notification auprès de la Commission européenne

15) Directive « services » : Le projet introduit-il une exigence en matière d'établissement ou de prestation de services transfrontalière ? ☐ Oui ☐ Non ☒ N.a. [2]

Si oui, veuillez contacter le Ministère de l'Economie en suivant les démarches suivantes :

https://meco.gouvernement.lu/fr/domaines-activites/politique-europeenne/notifications-directive-services.html

16) Directive « règles techniques » : Le projet introduit-il une exigence ou règlementation technique par rapport à un produit ou à un service de la société de l'information (domaine de la technologie et de l'information)? ☐ Oui ☐ Non ☒ N.a. [2]

Si oui, veuillez contacter l'ILNAS en suivant les démarches suivantes :

https://portail-qualite.public.lu/content/dam/qualite/publications/normalisation/2017/ilnas-notification-infoflyer-web.pdf