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.