Journal officiel
de l'Union européenne

FR
Série L

2025/2164

28.10.2025

DÉCISION D'EXÉCUTION (UE) 2025/2164 DE LA COMMISSION

du 27 octobre 2025

modifiant la décision d'exécution (UE) 2015/1505 en ce qui concerne la version de la norme sur laquelle se fonde le modèle commun de listes 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 22, paragraphe 5,

considérant ce qui suit:

(1) Les listes de confiance prévues à l'article 22, paragraphe 1, du règlement (UE) nº 910/2014 sont essentielles pour fonder la confiance des opérateurs économiques car elles permettent la validation du statut qualifié des prestataires de services de confiance et des services de confiance qu'ils fournissent. Par conséquent, il suffit aux prestataires de services de confiance qualifiés de commencer à fournir un service de confiance qualifié une fois que le statut qualifié est indiqué sur les listes de confiance.

(2) La décision d'exécution (UE) 2015/1505 de la Commission ([2]) établit les spécifications techniques et les formats relatifs aux listes de confiance. Ces spécifications et formats utilisent les spécifications et exigences énoncées dans la norme ETSI TS 119 612, version 2.1.1.

(3) Le règlement (UE) 2024/1183 du Parlement européen et du Conseil ([3]) a modifié le règlement (UE) nº 910/2014 en introduisant de nouveaux services de confiance qualifiés, à savoir la gestion de dispositifs de création de signature électronique qualifiés à distance, la gestion de dispositifs de création de cachet électronique qualifiés à distance, la délivrance d'attestations électroniques d'attributs qualifiées, la fourniture de services d'archivage électronique qualifiés et l'enregistrement de données électroniques dans un registre électronique qualifié. La norme ETSI TS 119 612 a été mise à jour dans la version 2.4.1 et contient désormais des spécifications permettant d'inclure et d'indiquer sur les listes de confiance le statut de ces nouveaux services de confiance qualifiés. La version 2.4.1 mise à jour a également modifié les spécifications relatives au format des signatures ou des cachets à utiliser par les États membres pour apposer une signature ou un cachet sur leurs listes de confiance nationales.

(4) Par conséquent, il convient de modifier la décision d'exécution (UE) 2015/1505 afin de mettre à jour la référence à la norme ETSI TS 119 612 dans sa version 2.4.1 plus récente. À la suite de cette modification, certaines adaptations supplémentaires s'imposent dans ladite décision d'exécution. Premièrement, les informations devant être mentionnées sur les listes de confiance, en ce qui concerne l'interprétation du contenu de ces listes, devraient être clarifiées afin de permettre aux parties utilisatrices d'interpréter les informations figurant sur lesdites listes de confiance. Deuxièmement, les spécifications relatives à la création des signatures ou cachets électroniques applicables aux listes de confiance devraient être adaptées afin d'éviter certaines vulnérabilités connues et signalées.

(5) Afin que les parties utilisatrices disposent de suffisamment de temps pour s'adapter aux spécifications figurant à l'annexe, il convient de différer l'application de la présente décision.

([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) 2015/1505 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).

([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).

(6) 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 de la présente décision.

(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 8 août 2025 ([7]).

(8) Les mesures prévues à la présente décision sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

L'annexe I de la décision d'exécution (UE) 2015/1505 est modifiée conformément à l'annexe de la présente décision.

Article 2

La présente décision entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

La présente décision d'exécution est applicable à partir du 29 avril 2026.

Fait à Bruxelles, le 27 octobre 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 regarding the version of the standard on which the common template of the trusted lists is based» (Commentaires formels du CEPD sur le projet concernant la version de la norme sur laquelle se fonde le modèle commun de listes de confiance) | Contrôleur européen de la protection des données.

ANNEXE

L'annexe I de la décision d'exécution (UE) 2015/1505 est modifiée comme suit:

1) Au chapitre II, le premier alinéa est remplacé par le texte suivant:

«Les présentes spécifications se fondent sur les spécifications et les prescriptions établies dans ETSI TS 119 612 v2.4.1 (ci-après dénommée ETSI TS 119 612).».

2) Au chapitre II, la section intitulée «Scheme type/community/rules (clause 5.3.9)» est remplacée par le texte suivant:

«**Scheme type/community/rules (clause 5.3.9)**

Ce champ est obligatoire et doit être conforme aux spécifications de la clause 5.3.9 d'ETSI TS 119 612.

Ce champ inclut seulement les URI anglais.

Ce champ comprend au moins deux URI:

1) un URI commun aux listes de confiance de tous les États membres pointant vers un texte descriptif qui doit s'appliquer à toutes les listes de confiance, comme suit:

— URI: http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon,

— Texte descriptif:

"A. ***Participation in a scheme***

Each Member State must create a trusted list including information related to the qualified trust service providers that are under supervision, together with information related to the qualified trust services they provide, in accordance with the relevant provisions laid down in Regulation (EU) N° 910/2014.

The present implementation of such trusted lists is also to be referred to in the list of links (pointers) towards each Member State's trusted list, compiled by the European Commission.

B. ***Policy/rules for the assessment of the listed services***

Member States must supervise qualified trust service providers established in the territory of the designating Member State as laid down in Chapter III of Regulation (EU) N° 910/2014 to ensure that those qualified trust service providers and the qualified trust services they provide meet the requirements laid down in that Regulation.

The trusted lists of Member States include, as a minimum, information specified in Articles 1 and 2 of Implementing Decision (EU) 2015/1505.

The trusted lists include both current and historical information about the status of listed trust services.

Each Member State's trusted list must provide information on the national supervisory scheme and, where applicable, national approval, including through accreditation scheme(s) under which the trust service providers and the trust services they provide are listed.

C. ***Interpretation of the trusted list***

The general user guidelines for applications, services or products relying on a trusted list published in accordance with Regulation (EU) N° 910/2014 are as follows:

C.1 ***Qualified status of a trust service***

The qualified status of a trust service is indicated by the combination of:

— the 'Service type identifier' ('Sti') value in a service entry,

— where applicable, the presence of one of the following values in all the fields 'additionalServiceInformation extension' in the service entry:

— 'http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures': further specifying the 'Sti' identified service as being provided for electronic signatures,

— 'http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals': further specifying the 'Sti' identified service as being provided for electronic seals, or

— 'http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication': further specifying the 'Sti' identified service as being provided for website authentication, and

— the status according to the 'Service current status' field value as from the date indicated in the 'Current status starting date and time'.

Historical information about such a qualified status is similarly provided when applicable.

C.1.1 ***Service status under Regulation (EU) Nº 910/2014***

Including and after 1 July 2016 (UTC+2), the value of the 'Service current status' field used by the Supervisory Body designated in a Member State to indicate that a trust service entry is representing a qualified trust service is the URI 'http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted'.

C.1.2 ***Service status under directive 1999/93/EC***

Strictly before 1st July 2016 (UTC+2), the value of the 'Service current status' field used by the Supervisory Body designated in a Member State to indicate that a trust service entry is representing a certification-service-provider issuing qualified certificates is one of the following URIs:

— 'http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision',

— 'http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation', or

— 'http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited'.

C.2 ***Qualified status of a certificate***

Regarding qualified trust service providers issuing qualified certificates for electronic signatures, for electronic seals and/or for website authentication, a 'CA/QC' 'Service type identifier' ('Sti') entry indicates that any end-entity certificate issued by or under the CA represented by the CA's public key and CA's name (both CA data to be considered as trust anchor input) present in the 'Service digital identifier' ('Sdi'), is or was a qualified certificate (QC) at a certain date and time provided that the trust service entry indicates a granted qualified status (see clause C.1) and that the below requirements are met with reference to that date and time.

C.2.1 ***Default rules***

C.2.1.1 *Certificate status standardised rule*

The end-entity certificate contains the ETSI standardised QcStatements extension as specified in standard ETSI EN 319 412-5 with the following requirements:

— the id-etsi-qcs-QcCompliance (urn:oid:0.4.0.1862.1.1) QcStatement is present, and

— where present, the id-etsi-qcs-QcType (urn:oid:0.4.0.1862.1.6) QcStatement contains exactly one of the following values:

  — the id-etsi-qct-esign (urn:oid:0.4.0.1862.6.1) ETSI defined QC type identifier,

  — the id-etsi-qct-eseal (urn:oid:0.4.0.1862.6.2) ETSI defined QC type identifier, or

  — the id-etsi-qct-web (urn:oid:0.4.0.1862.6.3) ETSI defined QC type identifier.

Optionally, the id-etsi-qct-QcSSCD (urn:oid:0.4.0.1862.4) QcStatement may be present.

C.2.1.2 *Certificate status under directive 1999/93/EC*

Restricted to the context of directive 1999/93/EC and as a legacy alternative to the above standardised rule, the end-entity certificate contains:

— the ETSI standardised QcStatements extension (as specified in ETSI EN 319 412-5) with the id-etsi-qcs-QcCompliance (urn:oid:0.4.0.1862.1.1) QcStatement being present,

— the legacy QCP+ (urn:oid:0.4.0.1456.1.1) ETSI defined certificate policy OID, or

— the legacy QCP (urn:oid:0.4.0.1456.1.2) ETSI defined certificate policy OID.

C.2.2 ***Additional rules: Presence of Qualifications Extension***

If 'Sie' 'Qualifications Extension' information as specified in clause 5.5.9.2 of standard ETSI TS 119 612 is present, then in addition to the above default rules, those certificates that are identified through the use of 'Sie' 'Qualifications Extension' information must be considered according to the associated qualifiers. Those qualifiers are used when necessary to compensate for a lack of standardised machine processable information in the corresponding certificate content. They are not to be used to compensate for a lack of machine processable information in certificates issued after 1 July 2016 where that lack would result in a non-compliance with Annex I, III or IV of Regulation (EU) N° 910/2014. However, they can be used to provide further machine processable information when the information provided in the certificate, while compliant with the Regulation, does not align with the above default interpretation rules. Where used, they provide additional information regarding:

— their qualified status:

  — 'QCStatement' ('http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCStatement') meaning the identified certificates are qualified under directive 1999/93/EC or under Regulation (EU) N° 910/2014, or

  — 'NotQualified' ('http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/NotQualified') meaning the identified certificates are not to be considered as qualified,

— the nature of their qualification:

  — 'QCForESig' ('http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig') meaning the identified certificates, when claimed or stated as qualified, are qualified certificates for electronic signature under Regulation (EU) N° 910/2014,

  — 'QCForESeal' ('http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESeal') meaning the identified certificates, when claimed or stated as qualified, are qualified certificates for electronic seal under Regulation (EU) N° 910/2014, or

  — 'QCForWSA' ('http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForWSA') meaning the identified certificates, when claimed or stated as qualified, are qualified certificates for website authentication under Regulation (EU) N° 910/2014,

— whether or not the private key resides in a qualified signature or qualified seal creation device (QSCD) and the nature thereof:

  — 'QCWithQSCD' ('http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD') meaning the identified certificates, when claimed or stated as qualified, have their private key residing in a QSCD,

  — 'QCNoQSCD' ('http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoQSCD') meaning the identified certificates, when claimed or stated as qualified, have not their private key residing in a QSCD,

  — 'QCQSCDStatusAsInCert' ('http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQSCDStatusAsInCert') meaning the identified certificates, when claimed or stated as qualified, do contain proper machine processable information about whether or not their private key is residing in a QSCD, or

  — 'QCQSCDManagedOnBehalf' ('http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQSCDManagedOnBehalf') meaning the identified certificates, when they are claimed or stated as qualified, have their private key is residing in a QSCD for which the generation and management of that private key is done by a qualified TSP on behalf of the entity whose identity is certified in the certificate.

Restricted to the context of certificates issued under directive 1999/93/EC, the following qualifiers are defined and provide additional information regarding:

— whether or not the private key resides in a secure signature creation device (SSCD):

  — 'QCWithSSCD' ('http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD') meaning the identified certificates, when claimed or stated as qualified, have their private key residing in an SSCD,

  — 'QCNoSSCD' ('http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoSSCD') meaning the identified certificates, when claimed or stated as qualified, do not have their private key residing in an SSCD, or

  — 'QCSSCDStatusAsInCert' ('http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCSSCDStatusAsInCert') meaning the identified certificates, when claimed or stated as qualified, do contain proper machine processable information about whether or not their private key is residing in an SSCD,

— the issuance to a Legal Person:

  — 'QCForLegalPerson' ('http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForLegalPerson') meaning the identified certificates, when claimed or stated as qualified, are issued to a Legal Person under directive 1999/93/EC.

Note: The information provided in the trusted list is to be considered as accurate meaning that the certificate is not to be considered as qualified if the end-entity certificate does not follow any of the default rules defined above, and:

  — if no 'Sie' 'Qualifications Extension' information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a 'QCStatement' qualifier, or

  — a 'Sie' 'Qualifications Extension' information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a 'NotQualified' qualifier.

C.3 *Trust anchors*

'Service digital identifiers' are to be used as Trust Anchors in the context of validating electronic signatures or seals for which signer's or seal creator's certificate is to be validated against information in the trusted list, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate represents the public key identifying the service, they are to be considered as Trust Anchor certificates conveying identical information with regard to the information strictly required as Trust Anchor information.

C.4 *General rule for the interpretation of trust service entries*

The general rule for interpretation of any 'Sti' type entry, possibly further specified through a 'Sie' 'additionalServiceInformation', not corresponding to qualified trust services is that, for that 'Sti' identified service type, and possibly in combination with a 'Sie' 'additionalServiceInformation' URI, the listed service named according to the 'Service name' field value and uniquely identified by the 'Service digital identity' field value has the current approval status according to the 'Service current status' field value as from the date indicated in the 'Current status starting date and time'.

Specific interpretation rules for any additional information with regard to a listed service (e.g. 'Service information extensions' field) may be found, when applicable, in the Member State specific URI as part of the present 'Scheme type/community/rules' field.

Please refer to the implementing acts adopted pursuant to Article 22(5) of Regulation (EU) N° 910/2014 for further details on the specifications of the fields of the Member States' trusted lists.

2) Un URI spécifique à la liste de confiance de chaque État membre pointant vers un texte descriptif qui doit s'appliquer à la liste de confiance dudit État membre:

a) http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC où CC = le code pays ISO 3166-1 ([1]) alpha-2 utilisé dans le champ 'Scheme territory' (clause 5.3.10)

— qui informe les utilisateurs des règles spécifiques à l'État membre en question selon lesquelles les services inclus sur la liste sont évalués conformément au système de contrôle et, le cas échéant, au système d'homologation dudit État membre,

— qui fournit aux utilisateurs une description spécifique de l'État membre en question quant à la manière d'utiliser et d'interpréter le contenu de la liste de confiance en ce qui concerne les services de confiance non qualifiés et/ou les services de confiance définis au niveau national répertoriés. Ce texte peut être utilisé pour indiquer que le système national d'homologation prévoit éventuellement un traitement distinct en ce qui concerne les CSP/TSP ne délivrant pas de QC et la manière dont le champ 'Scheme service definition URI' (clause 5.5.6) et le champ 'Service information extension' (clause 5.5.9) sont utilisés à cette fin.

b) Les États membres peuvent définir et utiliser des URI supplémentaires développant l'URI spécifique d'État membre (autrement dit, des URI définis à partir de cet URI hiérarchique).".».

3) Au chapitre II, après la section intitulée «Service current status (clause 5.5.4)», la section suivante est ajoutée:

«**L'élément Signature (clause B.1), Généralités (clause B.1.0)**

Cette clause est obligatoire et doit être conforme aux spécifications de la TS 119 612, clause B.1.0, où le point 2) est remplacé par le texte suivant:

"2) Son élément ds:SignedInfo doit contenir un élément ds:Reference dont l'attribut URI contient une chaîne de caractères vide (c'est-à-dire URI=''), de manière à renvoyer à l'ensemble du document. Cet élément ds:Reference doit satisfaire aux exigences suivantes:

a) il ne doit contenir qu'un seul élément ds:Transforms;

b) cet élément ds:Transforms doit contenir deux éléments ds:Transform. L'attribut Algorithm du premier indique la transformation enveloppée au moyen de la valeur suivante: 'http://www.w3.org/2000/09/xmldsig#enveloped-signature'. L'attribut Algorithm du second donne l'instruction d'effectuer la canonicalisation exclusive 'http://www.w3.org/2001/10/xml-exc-c14n#'.".».

([1]) ISO 3166-1:2006: Codes pour la représentation des noms de pays et de leurs subdivisions — Partie 1: Codes de pays.