2025/2164

28.10.2025

DECIZIA DE PUNERE ÎN APLICARE (UE) 2025/2164 A COMISIEI

din 27 octombrie 2025

de modificare a Deciziei de punere în aplicare (UE) 2015/1505 în ceea ce privește versiunea standardului pe care se bazează modelul comun al listelor sigure

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE ([1]), în special articolul 22 alineatul (5),

întrucât:

(1) Listele sigure prevăzute la articolul 22 alineatul (1) din Regulamentul (UE) nr. 910/2014 sunt esențiale pentru consolidarea încrederii în rândul operatorilor de piață, deoarece permit validarea statutului de calificat al prestatorilor de servicii de încredere și al serviciilor de încredere pe care le prestează. Prin urmare, prestatorii de servicii de încredere calificați trebuie să înceapă să presteze un serviciu de încredere calificat numai după ce statutul de calificat a fost indicat pe listele sigure.

(2) Decizia de punere în aplicare (UE) 2015/1505 a Comisiei ([2]) stabilește specificațiile tehnice și formatele pentru listele sigure. Aceste specificații și formate utilizează specificațiile și cerințele prevăzute în standardul ETSI TS 119 612 versiunea 2.1.1.

(3) Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului ([3]) a modificat Regulamentul (UE) nr. 910/2014 prin introducerea de noi servicii de încredere calificate, și anume gestionarea dispozitivelor calificate de creare a semnăturii electronice la distanță, gestionarea dispozitivelor calificate de creare a sigiliului electronic la distanță, emiterea de atestate electronice calificate ale atributelor, prestarea de servicii calificate de arhivare electronică și înregistrarea într-un registru electronic a datelor electronice și a documentelor în format electronic. Standardul ETSI TS 119 612 a fost actualizat la versiunea 2.4.1 și conține în prezent specificații care permit listelor sigure să includă și să indice statutul acestor noi servicii de încredere calificate. Versiunea actualizată 2.4.1 a modificat, de asemenea, specificațiile privind formatul semnăturilor sau al sigiliilor care trebuie utilizate de statele membre pentru semnarea sau sigilarea listelor lor sigure naționale.

(4) Prin urmare, Decizia de punere în aplicare (UE) 2015/1505 a Comisiei ar trebui modificată pentru a actualiza trimiterea la standardul ETSI TS 119 612 în versiunea sa mai recentă 2.4.1. Ca urmare a acestei modificări, sunt necesare, de asemenea, anumite modificări suplimentare ale deciziei de punere în aplicare respective. În primul rând, informațiile care trebuie să fie menționate în listele sigure, în ceea ce privește interpretarea conținutului unor astfel de liste, ar trebui clarificate pentru a le permite beneficiarilor să interpreteze informațiile din listele sigure. În al doilea rând, specificațiile referitoare la crearea semnăturilor sau sigiliilor electronice care trebuie să fie aplicate listelor sigure ar trebui adaptate pentru a preveni anumite vulnerabilități cunoscute și raportate.

(5) Pentru a se asigura că beneficiarii dispun de suficient timp pentru a se adapta la specificațiile prevăzute în anexă, aplicarea prezentei decizii ar trebui amânată.

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

([2]) Decizia de punere în aplicare (UE) 2015/1505 a Comisiei din 8 septembrie 2015 de stabilire a specificațiilor tehnice și a formatelor pentru listele sigure în temeiul articolului 22 alineatul (5) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă (JO L 235, 9.9.2015, p. 26, ELI: http://data.europa.eu/eli/dec_impl/2015/1505/oj).

([3]) Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului din 11 aprilie 2024 de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea cadrului european pentru identitatea digitală (JO L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([4]) și, după caz, Directiva 2002/58/CE a Parlamentului European și a Consiliului ([5]) se aplică tuturor activităților de prelucrare a datelor cu caracter personal efectuate în temeiul prezentei decizii.

(7) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([6]) și a emis un aviz la 8 august 2025 ([7]).

(8) Măsurile prevăzute în prezenta decizie sunt conforme cu avizul comitetului instituit prin articolul 48 din Regulamentul (UE) nr. 910/2014,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Anexa I la Decizia de punere în aplicare (UE) 2015/1505 se modifică în conformitate cu anexa la prezenta decizie.

Articolul 2

Prezenta decizie intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezenta decizie de punere în aplicare se aplică de la 29 aprilie 2026.

Adoptată la Bruxelles, 27 octombrie 2025.

Pentru Comisie
Președinta
Ursula VON DER LEYEN

([4]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 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 | European Data Protection Supervisor* (Observații formale ale AEPD cu privire la proiectul referitor la versiunea standardului pe care se bazează modelul comun al listelor sigure | Autoritatea Europeană pentru Protecția Datelor).

ANEXĂ

Anexa I la Decizia de punere în aplicare (UE) 2015/1505 se modifică după cum urmează:

1. În capitolul II, primul paragraf se înlocuiește cu următorul text:

„Prezentele specificații utilizează specificațiile și cerințele cuprinse în documentul intitulat «Specificațiile tehnice ale ETSI 119 612 v2.4.1» (denumit în continuare «ETSI TS 119 612»).”

2. În capitolul II, secțiunea de sub titlul „Scheme type/community/rules (Tipul/comunitatea/regulile programului) (secțiunea 5.3.9)” se înlocuiește cu următorul text:

„**Scheme type/community/rules (Tipul/comunitatea/regulile programului) (secțiunea 5.3.9)**

Acest câmp este obligatoriu și trebuie să respecte secțiunea 5.3.9 din ETSI TS 119 612.

Acest câmp trebuie să includă numai URI-uri în engleza britanică.

Acest câmp trebuie să conțină cel puțin două URI-uri:

1. Un URI comun tuturor listelor sigure ale statelor membre, care trimite la un text descriptiv aplicabil tuturor listelor sigure, după cum urmează:

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

   — Text descriptiv:

«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) No 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) No 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) No 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) No 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) No 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) No 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) No 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) No 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) No 910/2014 for further details on the specifications of the fields of the Member States' trusted lists.»

2. Un URI specific pentru fiecare listă sigură a unui stat membru care trimite la un text descriptiv aplicabil listei sigure a statului membru respectiv:

   (a) http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC unde CC = codul țării ISO 3166-1 ([1]) alpha-2 utilizat în câmpul «Scheme territory» (secțiunea 5.3.10)

   — unde utilizatorii găsesc politicile/regulile specifice ale statului membru respectiv, pe baza cărora sunt evaluate serviciile de încredere incluse în listă, în conformitate cu regimul de supraveghere al statului membru și, când este cazul, cu sistemul de omologare al acestuia;

   — unde utilizatorii găsesc o descriere specifică oferită de statul membru respectiv cu privire la modul de utilizare și de interpretare a conținutului listei sigure în ceea ce privește serviciile de încredere necalificate care figurează în listă și/sau serviciile de încredere definite la nivel național. Acesta poate fi utilizat pentru a indica o eventuală divizare în cadrul sistemului național de omologare în ceea ce privește CSP/TSP care nu eliberează QC și modul în care se utilizează «Scheme service definition URI» (secțiunea 5.5.6) și câmpul «Service information extension» (secțiunea 5.5.9) în acest scop.

   (b) Statele membre pot defini și utiliza URI-uri suplimentare prin extinderea URI-ului specific al statului membru, menționat mai sus (cu alte cuvinte URI-uri definite pornind de la acest URI ierarhic specific).”

3. În capitolul II, după secțiunea de sub titlul „Service current status (Statutul actual al serviciului) (secțiunea 5.5.4)”, se adaugă următoarea secțiune:

„**«Signature» element (Elementul «semnătură») (secțiunea B.1) – General (Aspecte generale) (secțiunea B.1.0)**

Această secțiune este obligatorie și trebuie să respecte secțiunea B.1.0 din TS 119 612, unde punctul 2 se înlocuiește cu următorul text:

„2. Elementul său «ds:SignedInfo» conține un element «ds:Reference» cu atributul URI stabilit la un șir gol (și anume URI=«»), astfel încât să se refere la întregul document. Acest element «ds:Reference» trebuie să îndeplinească următoarele cerințe:

   (a) trebuie să conțină doar un singur element «ds:Transforms»;

   (b) acest element «ds:Transforms» trebuie să conțină două elemente «ds:Transform». Primul va fi cel al cărui atribut al algoritmului indică transformarea de tip «enveloped» cu valoarea: «http://www.w3.org/2000/09/xmldsig#enveloped-signature». Al doilea va fi cel al cărui atribut al algoritmului impune efectuarea canonicalizării exclusive «http://www.w3.org/2001/10/xml-exc-c14n#».»”

([1]) ISO 3166-1:2006: «Coduri pentru reprezentarea denumirilor de țări și a subdiviziunilor lor. Partea 1: Codurile țărilor».