2025/2164

28.10.2025

KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2025/2164

af 27. oktober 2025

om ændring af gennemførelsesafgørelse (EU) 2015/1505 for så vidt angår versionen af den standard, på hvilken den fælles skabelon for positivlisterne er baseret

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF ([1]), særlig artikel 22, stk. 5, og

ud fra følgende betragtninger:

(1) Positivlister som omhandlet i artikel 22, stk. 1, i forordning (EU) nr. 910/2014 er afgørende for at opbygge tillid blandt markedsoperatørerne, da de gør det muligt at validere tillidstjenesteudbyderes og tillidstjenesters status som kvalificerede. Kvalificerede tillidstjenesteudbydere må derfor først udbyde en kvalificeret tillidstjeneste, når statussen som kvalificeret er opført på positivlisterne.

(2) I Kommissionens gennemførelsesafgørelse (EU) 2015/1505 ([2]) er der fastlagt tekniske specifikationer og formater for positivlister. Disse specifikationer og formater bygger på de specifikationer og krav, der er fastsat i standard ETSI TS 119 612 version 2.1.1.

(3) Med Europa-Parlamentets og Rådets forordning (EU) 2024/1183 ([3]) blev forordning (EU) nr. 910/2014 ændret, idet der blev indført nye kvalificerede tillidstjenester, nærmere bestemt forvaltning af kvalificerede elektroniske signaturgenereringssystemer på afstand, forvaltning af kvalificerede elektroniske seglgenereringssystemer på afstand, udstedelse af kvalificeret elektronisk attestering af attributter, levering af kvalificerede elektroniske arkiveringstjenester og registrering af elektroniske data i en kvalificeret elektronisk hovedbog. Standard ETSI TS 119 612 er blevet opdateret til version 2.4.1 og indeholder nu specifikationer, der gør det muligt at medtage og angive status for disse nye kvalificerede tillidstjenester på positivlister. I den opdaterede version 2.4.1 er specifikationerne for formatet for de signaturer eller segl, som medlemsstaterne skal anvende til at underskrive eller forsegle deres nationale positivlister, også blevet ændret.

(4) Kommissionens gennemførelsesafgørelse (EU) 2015/1505 bør derfor ændres for at ajourføre henvisningen til standard ETSI TS 119 612 til den nyere version 2.4.1. Som følge af denne ændring er der også behov for visse yderligere ændringer af nævnte gennemførelsesafgørelse. For det første bør de oplysninger, der skal henvises til i positivlisterne, angående hvordan indholdet af listerne skal fortolkes, gøres tydeligere, så modtagerparterne kan fortolke oplysningerne i positivlisterne. For det andet bør specifikationerne for generering af de elektroniske signaturer eller segl, der skal anvendes på positivlisterne, tilpasses for at forebygge visse kendte og indberettede sårbarheder.

(5) For at sikre, at modtagerparterne har tilstrækkelig tid til at tilpasse sig til specifikationerne i bilaget, bør anvendelsen af denne afgørelse udskydes.

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

([2]) Kommissionens gennemførelsesafgørelse (EU) 2015/1505 af 8. september 2015 om fastlæggelse af tekniske specifikationer og formater for positivlister i henhold til artikel 22, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked (EUT L 235 af 9.9.2015, s. 26, ELI: http://data.europa.eu/eli/dec_impl/2015/1505/oj).

([3]) Europa-Parlamentets og Rådets forordning (EU) 2024/1183 af 11. april 2024 om ændring af forordning (EU) nr. 910/2014 for så vidt angår fastlæggelse af den europæiske ramme for digital identitet (EUT L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([4]) og, hvor det er relevant, Europa-Parlamentets og Rådets direktiv 2002/58/EF ([5]) finder anvendelse på alle behandlingsaktiviteter vedrørende personoplysninger i henhold til denne afgørelse.

(7) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([6]) og afgav udtalelse den 8. august 2025 ([7]).

(8) Foranstaltningerne i denne afgørelse er i overensstemmelse med udtalelsen fra det udvalg, der er nedsat ved artikel 48 i forordning (EU) nr. 910/2014 —

VEDTAGET DENNE AFGØRELSE:

Artikel 1

Bilag I til gennemførelsesafgørelse (EU) 2015/1505 ændres som angivet i bilaget til nærværende afgørelse.

Artikel 2

Denne afgørelse træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne gennemførelsesafgørelse finder anvendelse fra den 29. april 2026.

Udfærdiget i Bruxelles, den 27. oktober 2025.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

([4]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EØS-relevant tekst) (EUT L 295 af 21.11.2018, s. 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 | Den Europæiske Tilsynsførende for Databeskyttelse.

BILAG

I bilag I til gennemførelsesafgørelse (EU) 2015/1505 foretages følgende ændringer:

(1) Kapitel II, første afsnit, affattes således:

»Nærværende specifikationer bygger på de specifikationer og krav, som er angivet i ETSI TS 119 612 v2.4.1 (herefter kaldet ETSI TS 119 612).«

(2) Kapitel II, afsnittet under overskriften »Scheme type/community/rules (clause 5.3.9)« affattes således:

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

This field shall be mandatory and shall comply with the specifications from ETSI TS 119 612 clause 5.3.9.

This field shall only include UK English URIs.

This field shall include at least two URIs:

(1) A URI common to all Member States' Trusted Lists pointing towards a descriptive text that shall be applicable to all Trusted Lists, as follows:

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

— Descriptive text:

»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) A URI specific to each Member State's trusted list pointing towards a descriptive text that shall be applicable to this Member State trusted list:

a) http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC where CC = the ISO 3166-1 ([1]) alpha-2 Country Code used in the »Scheme territory« field (clause 5.3.10)

— where users can obtain the referenced Member State's specific policies/rules against which trust services included in the list are assessed, in compliance with the Member State's supervisory regime and where applicable, approval scheme.

— where users can obtain a referenced Member State's specific description about how to use and interpret the content of the trusted list with regard to the listed non-qualified trust services and/or to nationally defined trust services. This may be used to indicate a potential granularity in the national approval system related to CSPs / TSPs not issuing QCs and how the »Scheme service definition URI« (clause 5.5.6) and the »Service information extension« field (clause 5.5.9) are used for this purpose.

b) Member States may define and use additional URIs expanding the above Member State specific URI (i.e. URIs defined from this hierarchical specific URI).«

(3) I kapitel II, efter afsnittet under overskriften »Service current status (punkt 5.5.4)«, tilføjes følgende afsnit:

»**The Signature element (clause B.1), General (clause B.1.0)**

Dette punkt er obligatorisk og skal være i overensstemmelse med specifikationerne fra TS 119 612, punkt B.1.0, hvori punkt 2) affattes således:

»2) Its ds:SignedInfo element shall contain a ds:Reference element with the URI attribute set to an empty string (i.e. URI=»"), so as to refer to the entire document. This ds:Reference element shall satisfy the following requirements:

a) It shall contain only one ds:Transforms element;

b) This ds:Transforms element shall contain two ds:Transform elements. The first one will be one whose Algorithm attribute indicates the enveloped transformation with the value: http://www.w3.org/2000/09/xmldsig#enveloped-signature}«. The second one will be one whose Algorithm attribute instructs to perform the exclusive canonicalization http://www.w3.org/2001/10/xml-exc-c14n#}«.«

([1]) ISO 3166-1:2006: »Codes for the representation of names of countries and their subdivisions Part 1: Country codes«.