Amtsblatt
der Europäischen Union

DE
Reihe L

2025/2164

28.10.2025

DURCHFÜHRUNGSBESCHLUSS (EU) 2025/2164 DER KOMMISSION

vom 27. Oktober 2025

zur Änderung des Durchführungsbeschlusses (EU) 2015/1505 in Bezug auf die Version der Norm, auf der die gemeinsame Vorlage für die Vertrauenslisten beruht

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG ([1]), insbesondere auf Artikel 22 Absatz 5,

in Erwägung nachstehender Gründe:

(1) Vertrauenslisten gemäß Artikel 22 Absatz 1 der Verordnung (EU) Nr. 910/2014 sind für den Aufbau von Vertrauen unter den Marktteilnehmern unverzichtbar, weil sie eine Validierung des Status qualifizierter Vertrauensdiensteanbieter und der von ihnen erbrachten Vertrauensdienste ermöglichen. Deshalb können qualifizierte Vertrauensdiensteanbieter erst dann mit der Erbringung eines qualifizierten Vertrauensdienstes beginnen, wenn der qualifizierte Status in den Vertrauenslisten ausgewiesen worden ist.

(2) Im Durchführungsbeschluss (EU) 2015/1505 der Kommission ([2]) sind technische Spezifikationen und Formate für Vertrauenslisten festgelegt worden. Diese Spezifikationen und Formate beruhen auf den Spezifikationen und Anforderungen der Norm ETSI TS 119 612 Version 2.1.1.

(3) Mit der Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates ([3]) wurde die Verordnung (EU) Nr. 910/2014 insofern geändert, dass neue qualifizierte Vertrauensdienste eingeführt wurden, nämlich für die Verwaltung qualifizierter elektronischer Fernsignaturerstellungseinheiten, die Verwaltung qualifizierter elektronischer Fernsiegelerstellungseinheiten, die Ausstellung qualifizierter elektronischer Attributsbescheinigungen, die Erbringung qualifizierter elektronischer Archivierungsdienste und die Aufzeichnung elektronischer Daten in einem qualifizierten elektronischen Journal. Die Norm ETSI TS 119 612 wurde auf die Version 2.4.1 aktualisiert und enthält nun Spezifikationen, die es ermöglichen, diese neuen qualifizierten Vertrauensdienste in die Vertrauenslisten aufzunehmen und ihren Status darin anzugeben. Mit der aktualisierten Version 2.4.1 wurden auch die Spezifikationen für das Format der Signaturen oder Siegel geändert, die von den Mitgliedstaaten zur Unterzeichnung oder Besiegelung ihrer nationalen Vertrauenslisten zu verwenden sind.

(4) Daher sollte der Durchführungsbeschluss (EU) 2015/1505 der Kommission geändert werden, um den Verweis auf die Norm ETSI TS 119 612 auf ihre neuere Version 2.4.1 zu aktualisieren. Infolge dieser Änderung sind noch bestimmte weitere Änderungen des genannten Durchführungsbeschlusses erforderlich. Erstens sollten die in den Vertrauenslisten aufzuführenden Informationen hinsichtlich der Auslegung des Inhalts solcher Listen präzisiert werden, damit vertrauende Beteiligte die Informationen in den Vertrauenslisten auslegen können. Zweitens sollten die Spezifikationen für die Erstellung der elektronischen Signaturen oder Siegel, die auf die Vertrauenslisten anzuwenden sind, angepasst werden, um bestimmte bekannte und gemeldete Schwachstellen zu beseitigen.

(5) Damit vertrauende Beteiligte ausreichend Zeit haben, sich auf die Spezifikationen des Anhangs einzustellen, sollte die Anwendung dieses Beschlusses verzögert werden.

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

([2]) Durchführungsbeschluss (EU) 2015/1505 der Kommission vom 8. September 2015 über technische Spezifikationen und Formate in Bezug auf Vertrauenslisten gemäß Artikel 22 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (ABl. L 235 vom 9.9.2015, S. 26, ELI: http://data.europa.eu/eli/dec_impl/2015/1505/oj).

([3]) Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität (ABl. L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([4]) und, sofern anwendbar, die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ([5]) gelten für jede Verarbeitung personenbezogener Daten gemäß dem vorliegenden Beschluss.

(7) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([6]) angehört und gab am 8. August 2025 seine Stellungnahme ab ([7]).

(8) Die in diesem Beschluss vorgesehenen Maßnahmen entsprechen der Stellungnahme des gemäß Artikel 48 der Verordnung (EU) Nr. 910/2014 eingesetzten Ausschusses —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Anhang I des Durchführungsbeschlusses (EU) 2015/1505 wird gemäß dem Anhang des vorliegenden Beschlusses geändert.

Artikel 2

Dieser Beschluss tritt am zwanzigsten Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Dieser Beschluss gilt ab dem 29. April 2026.

Brüssel, den 27. Oktober 2025

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

([4]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 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 | Europäischer Datenschutzbeauftragter.

ANHANG

Anhang I des Durchführungsbeschlusses (EU) 2015/1505 wird wie folgt geändert:

1. In Kapitel II erhält Absatz 1 folgende Fassung:
„Die vorliegenden Spezifikationen beruhen auf den in der Norm ETSI TS 119 612 Version 2.4.1 (im Folgenden ‚ETSI TS 119 612') festgelegten Spezifikationen und Anforderungen."

2. In Kapitel II erhält der Abschnitt unter der Überschrift „Systemart/Gemeinschaft/Regeln (Abschnitt 5.3.9)" folgende Fassung:

„**Systemart/Gemeinschaft/Regeln (Abschnitt 5.3.9)**

Dieses Feld ist obligatorisch und muss den Spezifikationen laut ETSI TS 119 612 Abschnitt 5.3.9 entsprechen.

Dieses Feld enthält ausschließlich URIs in britischem Englisch.

Dieses Feld enthält mindestens zwei URIs:

1. einen allen Vertrauenslisten der Mitgliedstaaten gemeinsamen URI, der zu einem deskriptiven Text führt, der für alle Vertrauenslisten gilt:

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

   — Deskriptiver 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. einen der Vertrauensliste eines Mitgliedstaats jeweils eigenen URI, der auf einen deskriptiven Text verweist, der für diese Vertrauensliste des Mitgliedstaats gilt:

   a) http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC; dabei ist CC der im Feld „Systemgebiet“ (Abschnitt 5.3.10) verwendete Alpha-2-Ländercode nach ISO 3166-1 ([1]), sowie

      — Angaben dazu, wo Nutzer länderspezifische Richtlinien/Vorschriften des betreffenden Mitgliedstaats finden können, anhand derer die in die Liste aufgenommenen Vertrauensdienste gemäß dem Aufsichtssystem und gegebenenfalls dem Genehmigungssystem des Mitgliedstaats bewertet werden.

      — Angaben dazu, wo Nutzer eine länderspezifische Anleitung des betreffenden Mitgliedstaats zur Verwendung und Auslegung des Inhalts der Vertrauensliste im Hinblick auf die aufgeführten nichtqualifizierten Vertrauensdienste und/oder auf nationaler Ebene definierten Vertrauensdienste finden können. Darin kann in Bezug auf Zertifizierungsdiensteanbieter bzw. Vertrauensdiensteanbieter, die keine qualifizierten Zertifikate ausstellen, auf eine potenzielle Granularität im einzelstaatlichen Genehmigungssystem hingewiesen und erläutert werden, wie die Felder ‚URI zur Definition des Systemdienstes‘ (Abschnitt 5.5.6) und ‚Dienstinformationserweiterung‘ (Abschnitt 5.5.9) zu diesem Zweck verwendet werden.

   b) Die Mitgliedstaaten können den obigen länderspezifischen URI erweitern, indem sie zusätzliche URIs definieren und verwenden (d. h. URIs, die auf diesem hierarchischen spezifischen URI basieren).“

3. In Kapitel II wird nach dem Abschnitt unter der Überschrift „Aktueller Dienststatus (Abschnitt 5.5.4)“ folgender Abschnitt angefügt:

„**Das Signaturelement (Abschnitt B.1) — Allgemeines (Abschnitt B.1.0)**

Dieses Feld ist obligatorisch und muss den Spezifikationen laut ETSI TS 119 612 Abschnitt B.1.0 entsprechen, wobei Nummer 2 folgende Fassung erhält:

‚2) Sein Element ds:SignedInfo muss ein Element ds:Reference enthalten, dessen URI-Attribut eine leere Zeichenfolge enthält (d. h. URI=""), damit es sich auf das gesamte Dokument bezieht. Dieses Element ds:Reference muss folgende Anforderungen erfüllen:

   a) Es darf nur ein Element ds:Transforms enthalten.

   b) Dieses Element ds:Transforms muss zwei Elemente ds:Transform enthalten. Das erste davon hat ein Algorithmus-Attribut, das die enveloped-Transformation mit dem folgenden Wert angibt: ‚http://www.w3.org/2000/09/xmldsig#enveloped-signature‘. Das zweite davon hat ein Algorithmus-Attribut, das die Durchführung der exklusiven Kanonisierung nach ‚http://www.w3.org/2001/10/xml-exc-c14n#‘ anweist.“‘

([1]) ISO 3166-1:2006: Codes für die Namen von Ländern und deren Untereinheiten — Teil 1: Codes für Ländernamen.