Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2025/2164

28.10.2025.

KOMISIJAS ĪSTENOŠANAS LĒMUMS (ES) 2025/2164

(2025. gada 27. oktobris)

par Īstenošanas lēmuma (ES) 2015/1505 grozījumiem attiecībā uz standarta redakciju, kas ir uzticamības sarakstu vienotās veidnes pamatā

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK ([1]), un jo īpaši tās 22. panta 5. punktu,

tā kā:

(1) Uzticamības saraksti, kas paredzēti Regulas (ES) Nr. 910/2014 22. panta 1. punktā, ir būtiski, lai veidotu uzticēšanos starp tirgus dalībniekiem, jo tie ļauj apstiprināt uzticamības pakalpojumu sniedzēju kvalifikācijas statusu un to sniegtos uzticamības pakalpojumus. Tāpēc kvalificēti uzticamības pakalpojumu sniedzēji var sākt sniegt kvalificētu uzticamības pakalpojumu pēc tam, kad uzticamības sarakstos ir norādīts kvalificētais statuss.

(2) Komisijas Īstenošanas lēmumā (ES) 2015/1505 ([2]) ir noteiktas uzticamības sarakstu tehniskās specifikācijas un formāti. Minētajās specifikācijās un formātos izmanto specifikācijas un prasības, kas noteiktas standarta ETSI TS 119 612 2.1.1. redakcijā.

(3) Ar Eiropas Parlamenta un Padomes Regulu (ES) 2024/1183 ([3]) tika grozīta Regula (ES) Nr. 910/2014, ieviešot jaunus kvalificētus uzticamības pakalpojumus, proti, attālinātu kvalificētu elektroniskā paraksta izveides ierīču pārvaldību, attālinātu kvalificētu elektroniskā zīmoga izveides ierīču pārvaldību, kvalificēta atribūtu elektroniskā apliecinājuma izdošanu, kvalificētu elektroniskās arhivēšanas pakalpojumu sniegšanu un elektronisko datu reģistrēšanu kvalificētā elektroniskajā virsgrāmatā. Standarts ETSI TS 119 612 ir atjaunināts uz 2.4.1. redakciju, un tagad tajā ir iekļautas specifikācijas, kas ļauj uzticamības sarakstos iekļaut šos jaunos kvalificētos uzticamības pakalpojumus un norādīt to statusu. Atjauninātajā 2.4.1. redakcijā ir grozītas arī specifikācijas attiecībā uz to parakstu vai zīmogu formātu, kas dalībvalstīm jāizmanto, lai parakstītu vai apzīmogotu savus valsts uzticamības sarakstus.

(4) Tāpēc Komisijas Īstenošanas lēmums (ES) 2015/1505 būtu jāgroza, lai atsauci uz standartu ETSI TS 119 612 atjauninātu ar tā jaunāko redakciju 2.4.1. Šā grozījuma rezultātā minētajā īstenošanas lēmumā ir vajadzīgas arī dažas papildu izmaiņas. Pirmkārt, būtu jāprecizē uzticamības sarakstos norādāmā informācija par šādu sarakstu satura interpretāciju, lai atkarīgās puses varētu interpretēt uzticamības sarakstos iekļauto informāciju. Otrkārt, specifikācijas, kas saistītas ar elektronisko parakstu vai zīmogu izveidi, kuras jāpiemēro uzticamības sarakstiem, būtu jāpielāgo, lai novērstu noteiktas zināmas un paziņotas ievainojamības.

(5) Lai nodrošinātu, ka atkarīgajām pusēm ir pietiekami daudz laika pielāgoties pielikumā izklāstītajām specifikācijām, šā lēmuma piemērošana būtu jāatliek.

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

([2]) Komisijas Īstenošanas lēmums (ES) 2015/1505 (2015. gada 8. septembris), kurā saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū 22. panta 5. punktu izklāstītas tehniskās specifikācijas un formāti, kas attiecas uz uzticamības sarakstiem (OV L 235, 9.9.2015., 26. lpp., ELI: http://data.europa.eu/eli/dec_impl/2015/1505/oj).

([3]) Eiropas Parlamenta un Padomes Regula (ES) 2024/1183 (2024. gada 11. aprīlis), ar ko groza Regulu (ES) Nr. 910/2014 attiecībā uz Eiropas digitālās identitātes satvara izveidi (OV L, 2024/1183, 30.4.2024., ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) Visām šajā lēmumā paredzētajām personas datu apstrādes darbībām piemēro Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 ([4]) un, attiecīgā gadījumā, Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK ([5]).

(7) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 ([6]) 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2025. gada 8. augustā sniedza savu atzinumu ([7]).

(8) Šajā lēmumā paredzētie pasākumi saskan ar atzinumu, ko sniegusi ar Regulas (ES) Nr. 910/2014 48. pantu izveidotā komiteja,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Īstenošanas lēmuma (ES) 2015/1505 I pielikumu groza tā, kā noteikts šā lēmuma pielikumā.

2. pants

Šis lēmums stājas spēkā divdesmitajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Šo Īstenošanas lēmumu piemēro no 2026. gada 29. aprīļa.

Briselē, 2025. gada 27. oktobrī

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

([4]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37. lpp., ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) EDAU oficiālas piezīmes par projektu attiecībā uz standarta redakciju, uz kuru balstās uzticamības sarakstu vienotā veidne | Eiropas Datu aizsardzības uzraudzītājs.

PIELIKUMS

Īstenošanas lēmuma (ES) 2015/1505 I pielikumu groza šādi:

1) II nodaļas pirmo daļu aizstāj ar šādu:

"Šajās specifikācijās izmanto specifikācijas un prasības, kas noteiktas ETSI TS 119 612 v2.4.1 (turpmāk "ETSI TS 119 612").";

2) II nodaļā iedaļu "*Scheme type/community/rules* (5.3.9. punkts)" aizstāj ar šādu:

"***Scheme type/community/rules* (5.3.9. punkts)**

Šis lauks ir obligāts un atbilst specifikācijām ETSI TS 119 612 5.3.9. punktā.

Šis lauks ietver URI tikai AK angļu valodā.

Šis lauks ietver vismaz divus URI:

1) vienu šādu URI, kas kopīgs visu dalībvalstu uzticamības sarakstiem un norāda uz aprakstošu tekstu, kurš piemērojams visiem uzticamības sarakstiem:

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

— Aprakstošais teksts:

"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) vienu URI, kas specifisks katras dalībvalsts uzticamības sarakstam un norāda uz aprakstošo tekstu, kurš piemērojams šās dalībvalsts uzticamības sarakstam:

a) http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, kur CC ir ISO 3166-1 ([1]) valsts divburtu kods, kas lietots laukā "Scheme territory" (5.3.10. punkts):

— kur lietotāji var iegūt ziņas par attiecīgās dalībvalsts īpašo politiku/noteikumiem, pēc kuriem tiek novērtēti sarakstā iekļautie uzticamības pakalpojumi atbilstoši dalībvalsts attiecīgajai pārraudzības sistēmai un – attiecīgos gadījumos – apstiprināšanas shēmai,

— kur lietotāji var iegūt attiecīgās dalībvalsts norādīto īpašo aprakstu par to, kā izmantot un interpretēt uzticamības saraksta saturu, kas attiecas uz sarakstā iekļautajiem nekvalificētajiem uzticamības pakalpojumiem un/vai valsts līmenī definētajiem uzticamības pakalpojumiem. To var izmantot, lai norādītu potenciālo granularitāti valsts apstiprināšanas sistēmās, kas saistītas ar *CSP/TSP*, kuri neizsniedz *QC*, un to, kā šim nolūkam izmanto laukus "Scheme service definition URI" (5.5.6. punkts) un "Service information extension" (5.5.9. punkts);

b) dalībvalstis var definēt un izmantot papildu URI, kas paplašina iepriekš norādīto dalībvalstij specifisko URI (t. i., URI, kas definēti no šā hierarhiskā specifiskā URI);

3) II nodaļā pēc iedaļas "*Service current status* (5.5.4. punkts)" pievieno šādu iedaļu:

"***The Signature element* (B.1. punkts), *General* (B.1.0. punkts)**

Šis punkts ir obligāts un atbilst specifikācijām TS 119 612 B.1.0. punktā, kur 2) punktu aizstāj ar šādu:

"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: "Valstu un to administratīvi teritoriālā iedalījuma vienību nosaukumu kodi. 1. daļa: Valstu kodi".