Europos Sąjungos
oficialusis leidinys

LT
L serija

2025/2164

2025 10 28

KOMISIJOS ĮGYVENDINIMO SPRENDIMAS (ES) 2025/2164

2025 m. spalio 27 d.

kuriuo dėl standarto, kuriuo grindžiama patikimų sąrašų bendroji forma, redakcijos iš dalies keičiamas Įgyvendinimo sprendimas (ES) 2015/1505

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentą (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB ([1]), ypač į jo 22 straipsnio 5 dalį,

kadangi:

(1) Reglamento (ES) Nr. 910/2014 22 straipsnio 1 dalyje numatyti patikimi sąrašai yra labai svarbūs didinant pasitikėjimą tarp rinkos operatorių, nes leidžia nustatyti patikimumo užtikrinimo paslaugų teikėjų ir jų teikiamų paslaugų kvalifikacijos statusą. Todėl kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai gali pradėti teikti kvalifikuotas patikimumo užtikrinimo paslaugas tik po to, kai kvalifikuotas statusas nurodomas patikimuose sąrašuose;

(2) Komisijos įgyvendinimo sprendime (ES) 2015/1505 ([2]) nustatytos patikimų sąrašų techninės specifikacijos ir formatai. Toms specifikacijoms ir formatams panaudotos standarte ETSI TS 119 612 (2.1.1 redakcija) pateiktos specifikacijos ir reikalavimai;

(3) Reglamentas (ES) Nr. 910/2014 iš dalies pakeistas Europos Parlamento ir Tarybos reglamentu (ES) 2024/1183 ([3]) – nustatytos naujos kvalifikuotos patikimumo užtikrinimo paslaugos, t. y. nuotolinių kvalifikuotų elektroninio parašo kūrimo įtaisų administravimas, nuotolinių kvalifikuotų elektroninio spaudo kūrimo įtaisų administravimas, kvalifikuotų elektroninių požymių liudijimų išdavimas, kvalifikuotų elektroninio archyvavimo paslaugų teikimas ir elektroninių duomenų įrašymas į kvalifikuotą elektroninį registrą. Standartas ETSI TS 119 612 buvo atnaujintas, todėl jo 2.4.1 redakcijoje dabar yra specifikacijos, kurių laikantis galima į patikimus sąrašus įrašyti ir juose nurodyti tas naująsias paslaugas. Atnaujintoje 2.4.1 redakcijoje taip pat iš dalies pakeistos parašų arba spaudų, kuriuos valstybės narės turi naudoti savo patikimiems sąrašams, formato specifikacijos;

(4) todėl Komisijos įgyvendinimo sprendimas (ES) 2015/1505 turėtų būti iš dalies pakeistas, kad jame būtų nurodyta naujesnė standarto ETSI TS 119 612 redakcija – 2.4.1. Dėl tokio pakeitimo taip pat reikia tam tikrų papildomų to įgyvendinimo sprendimo pakeitimų. Pirma, reikia paaiškinti patikimuose sąrašuose nurodomą informaciją, kiek tai susiję su tokių sąrašų turinio aiškinimu, kad patikimuose sąrašuose esančią informaciją galėtų suprasti pasikliaujančiosios šalys. Antra, reikėtų pagal poreikį pakeisti elektroninių parašų arba spaudų, naudojamų patikimuose sąrašuose, kūrimo specifikacijas siekiant apsisaugoti nuo tam tikro žinomo pažeidžiamumo arba pažeidžiamumo, apie kurį pranešta;

(5) kad pasikliaujančiosios šalys turėtų pakankamai laiko prisitaikyti prie naujų priede pateiktų specifikacijų, šio sprendimo taikymas turėtų būti atidėtas;

([1]) OL L 257, 2014 8 28, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) 2015 m. rugsėjo 8 d. Komisijos įgyvendinimo sprendimas (ES) 2015/1505, kuriuo pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje 22 straipsnio 5 dalį nustatomos patikimų sąrašų techninės specifikacijos ir formatai, (OL L 235, 2015 9 9, p. 26, ELI: http://data.europa.eu/eli/dec_impl/2015/1505/oj).

([3]) 2024 m. balandžio 11 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/1183, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 910/2014, kiek tai susiję su Europos skaitmeninės tapatybės sistemos nustatymu, (OL L, 2024/1183, 2024 4 30, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) visai asmens duomenų tvarkymo veiklai pagal šį sprendimą taikomi Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 ([4]) ir, kai aktualu, Europos Parlamento ir Tarybos direktyva 2002/58/EB ([5]);

(7) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([6]) 42 straipsnio 1 dalimi, konsultuotasi su Europos duomenų apsaugos priežiūros pareigūnu ir jis pateikė nuomonę 2025 m. rugpjūčio 8 d. ([7]);

(8) šiame sprendime nustatytos priemonės atitinka pagal Reglamento (ES) Nr. 910/2014 48 straipsnį įsteigto komiteto nuomonę,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Įgyvendinimo sprendimo (ES) 2015/1505 I priedas iš dalies keičiamas taip, kaip išdėstyta šio sprendimo priede.

2 straipsnis

Šis sprendimas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis įgyvendinimo sprendimas taikomas nuo 2026 m. balandžio 29 d.

Priimta Briuselyje 2025 m. spalio 27 d.

Komisijos vardu
Pirmininkė
Ursula VON DER LEYEN

([4]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas), (OL L 119, 2016 5 4, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), (OL L 201, 2002 7 31, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB, (OL L 295, 2018 11 21, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) Europos duomenų apsaugos priežiūros pareigūno oficialios pastabos dėl teisės akto projekto, kuriuo nustatoma patikimų sąrašų bendrosios formos pagrindinio standarto redakcija | Europos duomenų apsaugos priežiūros pareigūnas.

PRIEDAS

Įgyvendinimo sprendimo (ES) 2015/1505 I priedas iš dalies keičiamas taip:

1) II skyriaus pirma pastraipa pakeičiama taip:

„Šioms specifikacijoms panaudotos standarte ETSI TS 119 612 v2.4.1 (toliau – ETSI TS 119 612) pateiktos specifikacijos ir reikalavimai“;

2) II skyriaus skirsnis „Schemos tipas, naudotojai ir (arba) taisyklės (5.3.9 punktas)“ pakeičiamas taip:

„**Schemos tipas, naudotojai ir (arba) taisyklės (5.3.9 punktas)**

Šis laukas yra privalomas ir turi atitikti ETSI TS 119 612 5.3.9 punkte nustatytas specifikacijas.

Šiame lauke turi būti pateikti tik UII Jungtinės Karalystės anglų kalba.

Šiame lauke turi būti pateikti bent du UII:

1) visų valstybių narių patikimiems sąrašams bendras UII kaip nuoroda į aprašomąjį tekstą, kuris turi būti taikomas visiems patikimiems sąrašams:

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

   — aprašomasis tekstas:

„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 (ES) 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) specifinis kiekvienos valstybės narės patikimo sąrašo UII kaip nuoroda į aprašomąjį tekstą, kuris turi būti taikomas šios valstybės narės patikimam sąrašui:

a) http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, kur CC – ISO 3166-1 ([1]) dviejų raidžių šalies kodas, nurodytas lauke „Scheme territory“ („Schemos teritorija“) (5.3.10 punktas):

— šiame tekste naudotojai gali rasti informacijos apie konkrečias nurodytos valstybės narės politikos kryptis ir (arba) taisykles, pagal kurias, laikantis tos valstybės narės priežiūros režimo ir, kai taikytina, patvirtinimo schemos, vertinamos į sąrašą įtrauktos patikimos paslaugos,

— šiame tekste naudotojai gali rasti specifinį nurodytos valstybės narės aprašą, kaip naudoti ir aiškinti patikimo sąrašo turinį, susijusį su į sąrašą įtrauktomis nekvalifikuotomis patikimumo užtikrinimo paslaugomis ir (arba) nacionaliniu lygiu nustatytomis patikimumo užtikrinimo paslaugomis. Šis tekstas gali būti naudojamas galimam nacionalinių patvirtinimo sistemų, susijusių su kvalifikuotų sertifikatų neišduodančiais sertifikavimo paslaugų teikėjais / patikimumo užtikrinimo paslaugų teikėjais, hierarchijos lygiui nurodyti, taip pat nurodyti, kaip šiuo tikslu naudojami laukai „Pagal schemą teikiamos paslaugos apibrėžties UII“ (5.5.6 punktas) ir „Informacijos apie paslaugą plėtinys“ (5.5.9 punktas);

b) valstybės narės, praplėsdamos minėtą specifinį valstybės narės UII, gali nustatyti ir naudoti papildomus UII (t. y. UII, nustatomus remiantis šiuo specifiniu hierarchiniu UII).“;

3) po II skyriaus skirsnio „Dabartinis paslaugos statusas (5.5.4 punktas)“ įrašomas šis skirsnis:

„**Parašo elementas (B.1 punktas), bendrieji reikalavimai (B.1.0 punktas)**

Šis punktas yra privalomas ir turi atitikti TS 119 612 B.1.0 punkte nustatytas specifikacijas, kurių 2 punktas pakeičiamas taip:

2) jo elemente *ds:SignedInfo* turi būti elementas *ds:Reference*, kurio URI požymis yra tuščioji eilutė (t. y. URI=""), kad elementas būtų pritaikytas visam dokumentui. Toks elementas *ds:Reference* atitinka šiuos reikalavimus:

a) jis turi tik vieną elementą *ds:Transforms element*;

b) toks elementas *ds:Transforms element* turi du elementus *ds:Transform element*. Pirmasis elementas yra tas, kurio požymis *Algorithm* rodo apgaubtąją transformaciją, kurios vertė: „http://www.w3.org/2000/09/xmldsig#enveloped-signature“. Antrasis elementas yra tas, kurio požymis *Algorithm* rodo, kad reikia atlikti išskirtinį kanonizavimą: „http://www.w3.org/2001/10/xml-exc-c14n#“.“

([1]) ISO 3166-1:2006 „Šalių ir jų regionų pavadinimų kodai. 1 dalis. Šalių kodai“.