



VYKONÁVACIE ROZHODNUTIE KOMISIE (EÚ) 2025/2164

z 27. októbra 2025,

ktorým sa mení vykonávacie rozhodnutie (EÚ) 2015/1505, pokiaľ ide o verziu normy, z ktorej vychádza spoločný vzor pre dôveryhodné zoznamy

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES ⁽¹⁾, a najmä na jeho článok 22 ods. 5,

keďže:

- (1) Dôveryhodné zoznamy stanovené v článku 22 ods. 1 nariadenia (EÚ) č. 910/2014 sú nevyhnutné na budovanie dôvery medzi organizátormi trhu, keďže umožňujú validáciu kvalifikovaného štatútu poskytovateľov dôveryhodných služieb a dôveryhodných služieb, ktoré poskytujú. Kvalifikovaní poskytovatelia dôveryhodných služieb preto majú začať poskytovať kvalifikovanú dôveryhodnú službu až po tom, čo sa kvalifikovaný štatút uvedie v dôveryhodných zoznamoch.
- (2) Vykonávacím rozhodnutím Komisie (EÚ) 2015/1505 ⁽²⁾ sa ustanovujú technické špecifikácie a formáty týkajúce sa dôveryhodných zoznamov. Tieto špecifikácie a formáty využívajú špecifikácie a požiadavky stanovené vo verzii 2.1.1 normy ETSI TS 119 612.
- (3) Nariadením Európskeho parlamentu a Rady (EÚ) 2024/1183 ⁽³⁾ sa zmenilo nariadenie (EÚ) č. 910/2014 zavedením nových kvalifikovaných dôveryhodných služieb, konkrétne správy zariadení na vyhotovenie kvalifikovaného elektronického podpisu na diaľku, správy zariadení na vyhotovenie kvalifikovanej elektronickej pečate na diaľku, vydávania kvalifikovaného elektronického osvedčenia atribútov, poskytovania kvalifikovaných elektronických archivačných služieb a zaznamenávania elektronických údajov v kvalifikovanom elektronickej registri. Norma ETSI TS 119 612 bola aktualizovaná na verziu 2.4.1 a teraz obsahuje špecifikácie, ktoré umožňujú, aby zoznamy dôveryhodné zoznamy zahŕňali a uvádzali štatút týchto nových kvalifikovaných dôveryhodných služieb. Aktualizovanou verziou 2.4.1 sa zmenili aj špecifikácie formátu podpisov alebo pečatí, ktoré majú členské štáty používať na podpisovanie alebo zapečatenie svojich národných dôveryhodných zoznamov.
- (4) Vykonávacie rozhodnutie Komisie (EÚ) 2015/1505 by sa preto malo zmeniť s cieľom aktualizovať odkaz na normu ETSI TS 119 612 na jej novšiu verziu 2.4.1. V dôsledku tejto zmeny sú potrebné aj určité dodatočné zmeny uvedeného vykonávacieho rozhodnutia. Po prvé, informácie, ktoré sa majú uviesť v dôveryhodných zoznamoch, pokiaľ ide o výklad obsahu takýchto zoznamov, by sa mali objasniť, aby mohli spoľiehajúce sa strany vykladať informácie v dôveryhodných zoznamoch. Po druhé, špecifikácie týkajúce sa vytvárania elektronických podpisov alebo pečatí, ktoré sa majú uplatňovať na dôveryhodné zoznamy, by sa mali upraviť tak, aby sa zabránilo určitým známym a nahláseným zraniteľnostiam.
- (5) S cieľom zabezpečiť, aby spoľiehajúce sa strany mali dostatok času na prispôbenie sa špecifikáciám stanoveným v prílohe, by sa uplatňovanie tohto rozhodnutia malo odložiť.

⁽¹⁾ Ú. v. EÚ L 257, 28.8.2014, s. 73, ELI: <http://data.europa.eu/eli/reg/2014/910/oj>.

⁽²⁾ Vykonávacie rozhodnutie Komisie (EÚ) 2015/1505 z 8. septembra 2015, ktorým sa ustanovujú technické špecifikácie a formáty týkajúce sa dôveryhodných zoznamov podľa článku 22 ods. 5 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (Ú. v. EÚ L 235, 9.9.2015, s. 26, ELI: http://data.europa.eu/eli/dec_impl/2015/1505/oj).

⁽³⁾ Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1183 z 11. apríla 2024, ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o zriadenie európskeho rámca digitálnej identity (Ú. v. EÚ L, 2024/1183, 30.4.2024, ELI: <http://data.europa.eu/eli/reg/2024/1183/oj>).

- (6) Na všetky činnosti spracúvania osobných údajov podľa tohto rozhodnutia sa vzťahuje nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 (*) a v relevantných prípadoch smernica Európskeho parlamentu a Rady 2002/58/ES (†).
- (7) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 (‡) sa konzultovalo s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal 8. augusta 2025 svoje stanovisko (‡).
- (8) Opatrenia stanovené v tomto rozhodnutí sú v súlade so stanoviskom výboru uvedeného v článku 48 nariadenia (EÚ) č. 910/2014,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

Príloha I k vykonávaciemu rozhodnutiu (EÚ) 2015/1505 sa mení tak, ako sa uvádza v prílohe k tomuto rozhodnutiu.

Článok 2

Toto rozhodnutie nadobúda účinnosť dvadsiatym dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto vykonávacie rozhodnutie sa uplatňuje od 29. apríla 2026.

V Bruseli 27. októbra 2025

Za Komisiu
predsedníčka
Ursula VON DER LEYEN

(*) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).

(†) Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracúvania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, s. 37, ELI: <http://data.europa.eu/eli/dir/2002/58/oj>).

(‡) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

(§) EDPS *Formal comments on the draft regarding the version of the standard on which the common template of the trusted lists is based* (Formálne pripomienky EDPS k návrhu, pokiaľ ide o verziu normy, z ktorej vychádza spoločný vzor pre dôveryhodné zoznamy) [európsky dozorný úradník pre ochranu údajov].

PRÍLOHA

Príloha I k vykonávaciemu rozhodnutiu (EÚ) 2015/1505 sa mení takto:

1. V kapitole II sa prvý odsek nahrádza takto:
„Tieto špecifikácie sú založené na špecifikáciách a požiadavkách stanovených v norme ETSI TS 119 612 v2.4.1 (ďalej len „ETSI TS 119 612“).“
2. V kapitole II sa oddiel pod nadpisom „Typ schémy/komunity/pravidlá („Scheme type/community/rules“) (odsek 5.3.9)“ nahrádza takto:

„Typ schémy/komunity/pravidlá („Scheme type/community/rules“) (odsek 5.3.9)

Toto pole je povinné a je v súlade so špecifikáciami odseku 5.3.9 ETSI TS 119 612.

Toto pole zahŕňa len URI v britskej angličtine.

Toto pole zahŕňa minimálne dva URI:

1. URI spoločný pre všetky dôveryhodné zoznamy členských štátov, ktorý odkazuje na opisný text uplatniteľný na všetky dôveryhodné zoznamy nasledujúcim spôsobom:
 - URI: <http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon>
 - Opisný 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 schemes) 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. URI špecifický pre dôveryhodný zoznam každého členského štátu odkazujúci na opisný text, ktorý je uplatniteľný na dôveryhodný zoznam daného členského štátu:
 - a) <http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC>, kde CC = ISO 3166-1 ⁽¹⁾ alpha-2 kód krajiny používaný v poli „Scheme territory“ (odsek 5.3.10)
 - prostredníctvom tohto URI môžu používatelia získať prístup k osobitným politikám/pravidlám dotknutého členského štátu, podľa ktorých sa dôveryhodné služby na zozname posudzujú v súlade s režimom dohľadu daného členského štátu a v prípade potreby aj jeho schémou schvaľovania,
 - prostredníctvom tohto URI môžu používatelia získať prístup k osobitnému opisu členského štátu týkajúceho sa toho, ako používať a vykladať obsah dôveryhodného zoznamu vzhľadom na uvedené nekvalifikované dôveryhodné služby a/alebo dôveryhodné služby definované na vnútroštátnej úrovni. Toto sa môže využiť na znázornenie možnej nesúrodosti vnútroštátneho systému schvaľovania súvisiaceho s poskytovateľmi certifikovaných služieb/poskytovateľmi dôveryhodných služieb, ktorí nevydávajú kvalifikovaný certifikát, a na vysvetlenie, ako sa na tento účel používajú polia „Service definition URI“ (odsek 5.5.6) a „Service information extension“ (odsek 5.5.9);
 - b) členské štáty môžu vymedziť a používať dodatočný URI, ktorý je rozšírením uvedeného URI špecifického pre daný členský štát (t. j. URI vymedzený na základe tohto hierarchického špecifického URI).“
3. V kapitole II sa za oddiel pod nadpisom „Aktuálny štatút služby („Service current status“) (odsek 5.5.4)“ dopĺňa tento oddiel:

„Podpisový prvok („The Signature element“) (oddiel B.1), Všeobecne („General“) (oddiel B.1.0)

Tento oddiel je povinný a je v súlade so špecifikáciami oddielu B.1.0 TS 119 612, pričom bod 2) sa nahrádza takto:

- 2) Jeho prvok ds:SignedInfo obsahuje prvok ds:Reference s atribútom URI nastaveným na prázdny reťazec (t. j. URI=""), aby odkazoval na celý dokument. Tento prvok ds:Reference spĺňa nasledujúce požiadavky:
 - a) obsahuje len jeden prvok ds:Transforms;
 - b) tento prvok ds:Transforms obsahuje dva prvky ds:Transform. Prvým bude ten, ktorého atribút Algorithm odkazuje na transformáciu typu enveloped s hodnotou: "http://www.w3.org/2000/09/xmldsig#enveloped-signature)". Druhým bude ten, ktorého atribút Algorithm dáva pokyn na vykonanie exkluzívnej kanonikalizácie "http://www.w3.org/2001/10/xml-exc-c14n#)".“

⁽¹⁾ ISO 3166-1:2006: „Kódy na reprezentáciu názvov krajín a ich častí, 1. časť: Kódy krajín“.