Úřední věstník
Evropské unie

CS
Řada L

2025/2164

28.10.2025

PROVÁDĚCÍ ROZHODNUTÍ KOMISE (EU) 2025/2164

ze dne 27. října 2025,

kterým se mění prováděcí rozhodnutí (EU) 2015/1505, pokud jde o verzi normy, na níž je založena společná šablona důvěryhodných seznamů

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES ([1]), a zejména na čl. 22 odst. 5 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Důvěryhodné seznamy stanovené v čl. 22 odst. 1 nařízení (EU) č. 910/2014 mají zásadní význam pro budování důvěry mezi subjekty na trhu, neboť umožňují ověřit status kvalifikovaných poskytovatelů služeb vytvářejících důvěru a jimi poskytovaných kvalifikovaných služeb vytvářejících důvěru. Kvalifikovaní poskytovatelé služeb vytvářejících důvěru proto mohou začít danou kvalifikovanou službu vytvářející důvěru poskytovat až poté, co byl status kvalifikovaného poskytovatele nebo kvalifikované služby vyznačen v důvěryhodných seznamech.

(2) Prováděcí rozhodnutí Komise (EU) 2015/1505 ([2]) stanoví technické specifikace a formáty důvěryhodných seznamů. Tyto specifikace a formáty využívají specifikace a požadavky stanovené v normě ETSI TS 119 612 verzi 2.1.1.

(3) Nařízení Evropského parlamentu a Rady (EU) 2024/1183 ([3]) změnilo nařízení (EU) č. 910/2014 zavedením nových kvalifikovaných služeb vytvářejících důvěru, a to správy kvalifikovaných prostředků pro vytváření elektronických podpisů na dálku, správy kvalifikovaných prostředků pro vytváření elektronických pečetí na dálku, vydávání kvalifikovaných elektronických potvrzení atributů, poskytování kvalifikovaných služeb elektronické archivace a zaznamenávání elektronických dat do kvalifikované elektronické knihy záznamů. Norma ETSI TS 119 612 byla aktualizována na verzi 2.4.1 a nyní obsahuje specifikace, které umožňují zahrnout do důvěryhodných seznamů tyto nové kvalifikované služby vytvářející důvěru a vyznačit v nich jejich status. Aktualizovaná verze 2.4.1 rovněž změnila specifikace pro formát podpisů nebo pečetí, které mají členské státy používat k podepisování nebo pečetění svých vnitrostátních důvěryhodných seznamů.

(4) Prováděcí rozhodnutí Komise (EU) 2015/1505 by proto mělo být změněno tak, aby byl aktualizován odkaz na normu ETSI TS 119 612 na její novější verzi 2.4.1. V důsledku této změny je rovněž nutné provést některé další změny uvedeného prováděcího rozhodnutí. Za prvé, informace, které mají být uvedeny v důvěryhodných seznamech, pokud jde o výklad obsahu těchto seznamů, by měly být vyjasněny, aby spoléhající se strany mohly informace v důvěryhodných seznamech interpretovat. Za druhé, specifikace týkající se vytváření elektronických podpisů nebo pečetí, které mají být uplatněny na důvěryhodné seznamy, by měly být upraveny tak, aby se zabránilo některým známým a nahlášeným slabým místům.

(5) Aby měly spoléhající se strany dostatek času na přizpůsobení se specifikacím uvedeným v příloze, mělo by být uplatňování tohoto rozhodnutí odloženo.

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

([2]) Prováděcí rozhodnutí Komise (EU) 2015/1505 ze dne 8. září 2015, kterým se stanoví technické specifikace a formáty důvěryhodných seznamů podle čl. 22 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (Úř. věst. L 235, 9.9.2015, s. 26, ELI: http://data.europa.eu/eli/dec_impl/2015/1505/oj).

([3]) Nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu (Úř. věst. L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) Na všechny činnosti zpracování osobních údajů podle tohoto rozhodnutí se vztahuje nařízení Evropského parlamentu a Rady (EU) 2016/679 ([4]) a v příslušných případech směrnice Evropského parlamentu a Rady 2002/58/ES ([5]).

(7) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([6]) byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 8. srpna 2025 ([7]).

(8) Opatření stanovená tímto rozhodnutím jsou v souladu se stanoviskem výboru zřízeného článkem 48 nařízení (EU) č. 910/2014,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

Příloha I prováděcího rozhodnutí (EU) 2015/1505 se mění v souladu s přílohou tohoto rozhodnutí.

Článek 2

Toto rozhodnutí vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto prováděcí rozhodnutí se použije ode dne 29. dubna 2026.

V Bruselu dne 27. října 2025.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

([4]) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) (Úř. věst. L 201, 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) Nařízení Evropského Parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) Formální připomínky EIOÚ k návrhu týkajícímu se verze normy, na níž je založena společná šablona důvěryhodných seznamů | evropský inspektor ochrany údajů.

PŘÍLOHA

Příloha I prováděcího rozhodnutí (EU) 2015/1505 se mění takto:

1) V kapitole II se první odstavec nahrazuje tímto:

„Tyto specifikace využívají specifikace a požadavky stanovené v ETSI TS 119 612 v2.4.1 (dále jen „ETSI TS 119 612).“

2) V kapitole II se oddíl s názvem „Typ systému/komunita/pravidla (Scheme type/community/rules) (bod 5.3.9)“ nahrazuje tímto:

„**Typ systému/komunita/pravidla (Scheme type/community/rules) (bod 5.3.9)**

Toto pole je povinné a je v souladu se specifikacemi ETSI TS 119 612 bodem 5.3.9.

Toto pole zahrnuje pouze jednotné identifikátory zdroje (URI) v britské angličtině.

Toto pole zahrnuje nejméně dva identifikátory URI:

1) URI společný pro všechny důvěryhodné seznamy členských států, který odkazuje na popisný text, jenž se vztahuje na všechny důvěryhodné seznamy, viz níže:

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

— Popisný 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 URIhttp://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 specifický pro každý důvěryhodný seznam členského státu odkazující na popisný text, který se vztahuje na důvěryhodný seznam tohoto členského státu:

a) http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, kde CC = dvoupísmenný kód země podle ISO 3166-1 ([1]) použitý v poli „Scheme territory“ (bod 5.3.10),

— kde mohou uživatelé získat specifické politiky/pravidla příslušného členského státu, podle nichž jsou služby vytvářející důvěru uvedené na seznamu posuzovány z hlediska souladu se systémem dohledu a v příslušných případech schvalovacím systémem členského státu,

— kde mohou uživatelé získat specifický popis vypracovaný příslušným členským státem o tom, jak používat a vykládat obsah důvěryhodného seznamu s ohledem na nekvalifikované služby vytvářející důvěru uvedené na seznamu a/nebo na vnitrostátně definované služby vytvářející důvěru. Toho lze využít k poukázání na možnou nesourodost mezi vnitrostátními schvalovacími systémy souvisejícími s ověřovateli / poskytovateli služeb vytvářejících důvěru nevydávajícími kvalifikované certifikáty a tím, jak jsou pro tyto účely využívána pole „Scheme service definition URI“ (bod 5.5.6) a „Service information extension“ (bod 5.5.9);

b) členské státy mohou definovat a používat další URI, které jsou rozšířením výše uvedeného URI specifického pro jednotlivé členské státy (tj. URI definované na základě tohoto hierarchického specifického URI).“

3) V kapitole II se za oddíl s názvem „Aktuální status služby (Service current status) (bod 5.5.4)“ doplňuje nový oddíl, který zní:

„**Prvek podpisu (The Signature element) (bod B.1), Obecně (General) (bod B.1.0)**

Tento bod je povinný a je v souladu se specifikacemi normy TS 119 612 bodem B.1.0, kde se bod 2) nahrazuje tímto:

„2) Prvek ds:SignedInfo obsahuje prvek ds:Reference s atributem URI nastaveným na prázdný řetězec (tj. URI=""), aby odkazoval na celý dokument. Tento prvek ds:Reference splňuje následující požadavky:

a) obsahuje pouze jeden prvek ds:Transforms;

b) tento prvek ds:Transforms obsahuje dva prvky ds:Transform. Prvním z nich bude ten, jehož atribut Algorithm odkazuje na transformaci typu enveloped s hodnotou: „http://www.w3.org/2000/09/xmldsig#enveloped-signature“. Druhým bude ten, jehož atribut Algorithm nařizuje provést výhradní kanonizaci, „http://www.w3.org/2001/10/xml-exc-c14n#“.““

([1]) ISO 3166-1:2006: „Kódy pro názvy zemí a jejich částí – Část 1: Kódy zemí“.