2025/2164

28.10.2025 г.

РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2025/2164 НА КОМИСИЯТА

от 27 октомври 2025 година

за изменение на Решение за изпълнение (ЕС) 2015/1505 по отношение на версията на стандарта, на който се основава общият образец за доверителните списъци

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО ([1]), и по-специално член 22, параграф 5 от него,

като има предвид, че:

(1) Доверителните списъци, предвидени в член 22, параграф 1 от Регламент (ЕС) № 910/2014, са от съществено значение за изграждането на доверие между операторите на пазара, тъй като позволяват валидиране на квалифицирания статус на доставчиците на удостоверителни услуги и на предоставяните от тях удостоверителни услуги. Следователно доставчиците на квалифицирани удостоверителни услуги могат да започнат да предоставят квалифицирана удостоверителна услуга едва след като квалифицираният статус бъде отбелязан в доверителните списъци.

(2) С Решение за изпълнение (ЕС) 2015/1505 ([2]) на Комисията се определят техническите спецификации и форматите, свързани с доверителните списъци. Тези спецификации и формати се основават на спецификациите и изискванията, определени в стандарта ETSI TS 119 612, версия 2.1.1.

(3) С Регламент (ЕС) 2024/1183 на Европейския парламент и на Съвета ([3]) беше изменен Регламент (ЕС) № 910/2014, като бяха въведени нови квалифицирани удостоверителни услуги, а именно управлението на устройства за създаване на квалифициран електронен подпис от разстояние, управлението на устройства за създаване на квалифициран електронен печат от разстояние, издаването на квалифицирано електронно удостоверение за атрибути, предоставянето на квалифицирани услуги за електронно архивиране и записването на електронни данни в квалифициран електронен регистър. Стандартът ETSI TS 119 612 е актуализиран до версия 2.4.1 и понастоящем съдържа спецификации, които позволяват на доверителните списъци да включват и посочват статуса на тези нови квалифицирани удостоверителни услуги. Актуализираната версия 2.4.1 също така измени спецификациите за формàта на подписите или печатите, които да се използват от държавите членки за подписване или подпечатване на техните национални доверителни списъци.

(4) Поради това Решение за изпълнение (ЕС) 2015/1505 на Комисията следва да бъде изменено, за да се актуализира позоваването на стандарт ETSI TS 119 612 с неговата по-нова версия 2.4.1. В резултат на това изменение са необходими и някои допълнителни промени в посоченото решение за изпълнение. Първо, информацията, която трябва да бъде посочена в доверителните списъци, що се отнася до тълкуването на съдържанието на тези списъци, следва да бъде изяснена, за да могат доверяващите се страни да тълкуват информацията в доверителните списъци. Второ, спецификациите, свързани със създаването на електронните подписи или печати, които трябва да се прилагат към доверителните списъци, следва да бъдат адаптирани, за да се предотвратят някои известни и докладвани уязвимости.

(5) За да се гарантира, че доверяващите се страни разполагат с достатъчно време, за да се адаптират към спецификациите, посочени в приложението, прилагането на настоящото решение следва да бъде отложено.

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

([2]) Решение за изпълнение (ЕС) 2015/1505 на Комисията от 8 септември 2015 година за определяне на техническите спецификации и форматите на доверителните списъци съгласно член 22, параграф 5 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар (ОВ L 235, 9.9.2015 г., стр. 26, ELI: http://data.europa.eu/eli/dec_impl/2015/1505/oj).

([3]) Регламент (ЕС) 2024/1183 на Европейския парламент и на Съвета от 11 април 2024 г. за изменение на Регламент (ЕС) № 910/2014 по отношение на създаването на европейска рамка за цифрова самоличност (ОВ L, 2024/1183, 30.4.2024 г., ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([4]) и, когато е целесъобразно, Директива 2002/58/ЕО на Европейския парламент и на Съвета ([5]) се прилагат по отношение на всички дейности по обработване на лични данни съгласно настоящото решение.

(7) Европейският надзорен орган по защита на данните беше консултиран в съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([6]) и прие своето становище на 8 август 2025 г. ([7])

(8) Мерките, предвидени в настоящото решение, са в съответствие със становището на комитета, създаден съгласно член 48 от Регламент (ЕС) № 910/2014,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Приложение I към Решение за изпълнение (ЕС) 2015/1505 се изменя, както е определено в приложението към настоящото решение.

Член 2

Настоящото решение влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

Настоящото решение за изпълнение се прилага от 29 април 2026 г.

Съставено в Брюксел на 27 октомври 2025 година.

За Комисията
Председател
Ursula VON DER LEYEN

([4]) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации), (ОВ L 201, 31.7.2002 г., стр. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (ОВ L 295, 21.11.2018 г., стр. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) Официални коментари на ЕНОЗД по проекта относно версията на стандарта, на който се основава общият образец на доверителните списъци | Европейски надзорен орган по защита на данните.

ПРИЛОЖЕНИЕ

Приложение I към Решение за изпълнение (ЕС) 2015/1505 се изменя, както следва:

1) В глава II първият параграф се заменя със следното:

„Настоящите спецификации подсилват спецификациите и изискванията, определени в ETSI TS 119 612 v2.4.1 (наричани по-долу „ETSI TS 119 612“)“.

2) В глава II разделът под заглавието „Тип/общност/правила на схемата (клауза 5.3.9)“ се заменя със следното:

„**Scheme type/community/rules („Тип/общност/правила на схемата“) (клауза 5.3.9)**

Това поле е задължително и трябва да съответства на спецификациите в клауза 5.3.9 от ETSI TS 119 612.

То включва само URI на британски английски.

То включва най-малко два URI:

1) общ URI за доверителните списъци на всички държави членки, насочващ към описателен текст, който да е приложим за всички доверителни списъци, както следва:

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

— Описателен текст:

„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) № 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) № 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) № 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) № 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 trust service***

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 *Service 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) № 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) № 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) № 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) № 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) № 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

  — an „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) № 910/2014 for further details on the specifications of the fields of the Member States' trusted lists.“

2) Специфичен за доверителния списък на всяка държава членка идентификатор (URI), насочващ към описателен текст, който се отнася за доверителния списък на тази държава членка:

а) http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, където CC = двубуквеният код на държавата по ISO 3166-1 ([1]) [2], използван в полето „Scheme territory“ („Територия на схемата“) (точка 5.3.10.)

— там потребителите могат да намерят специфичните за съответната държава членка политики/правила, съгласно които се оценяват включените в списъка услуги в съответствие с нейния режим за надзор и, когато е приложимо, схема за одобряване.

— там потребителите могат да намерят специфично за дадената държава членка описание как да използват и тълкуват съдържанието на доверителния списък по отношение на вписаните неквалифицирани удостоверителни услуги и/или удостоверителните услуги, определени на национално равнище. Описанието може да се използва за указване на евентуална нееднородност в националната система за одобряване по отношение на доставчици на услуги по сертифициране/доставчици на удостоверителни услуги, които не издават квалифицирани удостоверения (КУ), както и на начина, по който „Scheme service definition URI“ (клауза 5.5.6) и полето „Service information extension“ (клауза 5.5.9) се използват за тази цел.

б) Държавите членки може да определят и използват допълнителни URI, разширяващи горепосочения специфичен за държавата членка URI (т.е. URI, попадащи в йерархията на този специфичен URI).“

3) В глава II след раздела под заглавието „Service current status“ („Актуално състояние на услугата“) (клауза 5.5.4) се добавя следният раздел:

„**The Signature element (clause B.1), General (clause B.1.0) (Елемент подпис (клауза B.1), Общи (клауза B.1.0)**

Тази точка е задължителна и съответства на спецификациите от TS 119 612, клауза B.1.0, където точка 2 се заменя със следното:

„2) неговият ds:SignedInfo елемент трябва да съдържа ds:Reference елемент с атрибут URI, съдържащ празен низ (т.е. URI = „“), така че да се отнася за целия документ. Този ds:Reference елемент трябва да отговаря на следните изисквания:

а) Той съдържа само един ds:Transforms елемент;

б) Този ds:Transforms елемент трябва да съдържа два ds:Transform елемента. Първият е този, чийто атрибут Algorithm указва пакетната трансформация със стойност: „http://www.w3.org/2000/09/xmldsig#enveloped-signature}“. Вторият е този, чийто атрибут Algorithm съдържа указание за извършване на exclusive canonicalization съгласно „http://www.w3.org/2001/10/xml-exc-c14n#}“.““

([1]) ISO 3166-1:2006: „Кодове за представяне на наименованията на държавите и техните подразделения. Част 1: Кодове на държавите“.