2025/2164

28.10.2025

DECYZJA WYKONAWCZA KOMISJI (UE) 2025/2164

z dnia 27 października 2025 r.

zmieniająca decyzję wykonawczą (UE) 2015/1505 w odniesieniu do wersji normy, na której opiera się wspólny wzór zaufanych list

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE ([1]), w szczególności jego art. 22 ust. 5,

a także mając na uwadze, co następuje:

(1) Zaufane listy przewidziane w art. 22 ust. 1 rozporządzenia (UE) nr 910/2014 mają zasadnicze znaczenie dla procesu budowania zaufania wśród operatorów rynku, ponieważ umożliwiają walidację kwalifikowanego statusu dostawców usług zaufania i świadczonych przez nich usług zaufania. W związku z tym kwalifikowani dostawcy usług zaufania mają rozpoczynać świadczenie kwalifikowanej usługi zaufania dopiero po tym, jak ich status kwalifikowany zostanie wskazany na zaufanych listach.

(2) W decyzji wykonawczej Komisji (UE) 2015/1505 ([2]) ustanowiono specyfikacje techniczne i formaty dotyczące zaufanych list. Te specyfikacje i formaty wykorzystują specyfikacje i wymogi określone w normie ETSI TS 119 612 wersja 2.1.1.

(3) Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1183 ([3]) zmieniono rozporządzenie (UE) nr 910/2014 poprzez wprowadzenie nowych kwalifikowanych usług zaufania, a mianowicie usług zarządzania kwalifikowanymi urządzeniami do składania podpisu elektronicznego na odległość, zarządzania kwalifikowanymi urządzeniami do składania pieczęci elektronicznej na odległość, wydawania kwalifikowanych elektronicznych poświadczeń atrybutów, świadczenia kwalifikowanych usług archiwizacji elektronicznej oraz rejestrowania danych elektronicznych w kwalifikowanym rejestrze elektronicznym. Normę ETSI TS 119 612 zaktualizowano do wersji 2.4.1 i obecnie zawiera ona specyfikacje umożliwiające uwzględnienie tych nowych kwalifikowanych usług zaufania i wskazanie statusu w zaufanych listach. W zaktualizowanej wersji 2.4.1 zmieniono również specyfikacje dotyczące formatu podpisów lub pieczęci, które mają być stosowane przez państwa członkowskie do podpisywania lub pieczętowania swoich krajowych zaufanych list.

(4) Należy zatem zmienić decyzję wykonawczą Komisji (UE) 2015/1505, aby zaktualizować odniesienie do normy ETSI TS 119 612 do jej nowszej wersji 2.4.1. W wyniku tej zmiany konieczne są również pewne dodatkowe zmiany we wspomnianej decyzji wykonawczej. Po pierwsze, należy doprecyzować informacje, które mają być podane w zaufanych listach w odniesieniu do interpretacji treści tych list, aby umożliwić stronom ufającym interpretację informacji zawartych w zaufanych listach. Po drugie, należy dostosować specyfikacje dotyczące tworzenia podpisów elektronicznych lub pieczęci elektronicznych, które mają być stosowane w odniesieniu do zaufanych list, aby zapobiec niektórym znanym i zgłaszanym podatnościom na ryzyko.

(5) W celu zapewnienia, aby strony ufające miały wystarczająco dużo czasu na dostosowanie się do specyfikacji określonych w załączniku, stosowanie niniejszej decyzji powinno zostać odłożone w czasie.

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

([2]) Decyzja wykonawcza Komisji (UE) 2015/1505 z dnia 8 września 2015 r. ustanawiająca specyfikacje techniczne i formaty dotyczące zaufanych list zgodnie z art. 22 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz.U. L 235 z 9.9.2015, s. 26, ELI: http://data.europa.eu/eli/dec_impl/2015/1505/oj).

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (Dz.U. L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 ([4]) oraz – w stosownych przypadkach – dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady ([5]) mają zastosowanie do wszystkich czynności przetwarzania danych osobowych na podstawie niniejszej decyzji.

(7) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([6]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 8 sierpnia 2025 r. ([7]).

(8) Środki przewidziane w niniejszej decyzji są zgodne z opinią komitetu ustanowionego na podstawie art. 48 rozporządzenia (UE) nr 910/2014,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

W załączniku I do decyzji wykonawczej (UE) 2015/1505 wprowadza się zmiany zgodnie z załącznikiem do niniejszej decyzji.

Artykuł 2

Niniejsza decyzja wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejszą decyzję wykonawczą stosuje się od dnia 29 kwietnia 2026 r.

Sporządzono w Brukseli dnia 27 października 2025 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) Formalne uwagi EIOD do projektu dotyczącego wersji normy, na której opiera się wspólny wzór zaufanych list | Europejski Inspektor Ochrony Danych.

ZAŁĄCZNIK

W załączniku I do decyzji wykonawczej (UE) 2015/1505 wprowadza się następujące zmiany:

1) w rozdziale II akapit pierwszy otrzymuje brzmienie:
„Niniejsza specyfikacja opiera się na specyfikacji i wymogach określonych w ETSI TS 119 612 v2.4.1 (zwanej dalej ETSI TS 119 612).";

2) w rozdziale II sekcja pod tytułem „Scheme type/community/rules (rodzaj systemu/wspólnota/zasady) (klauzula 5.3.9)" otrzymuje brzmienie:

„**Scheme type/community/rules (rodzaj systemu/wspólnota/zasady) (klauzula 5.3.9)**

Pole to jest obowiązkowe i musi być zgodne ze specyfikacjami zawartymi w klauzuli 5.3.9 ETSI TS 119 612.

Pole to zawiera URI wyłącznie w języku angielskim (ZK).

Pole to zawiera co najmniej dwa URI:

1) URI wspólny dla zaufanych list wszystkich państw członkowskich wskazujący tekst opisowy, który musi mieć zastosowanie do wszystkich zaufanych list, w brzmieniu:

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

— Tekst opisowy:

»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 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 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

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

2) URI określony dla zaufanej listy każdego państwa członkowskiego wskazujący na tekst opisowy, który musi mieć zastosowanie do zaufanej listy tego państwa członkowskiego:

   a) http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, w którym CC = kod kraju zgodny z ISO 3166-1 ([1]) alfa-2 umieszczany w polu »Scheme territory« (klauzula 5.3.10),

      — gdzie użytkownicy mogą uzyskać dostęp do określonych polityk/zasad danego państwa członkowskiego, na których podstawie usługi zaufania zawarte na liście są oceniane zgodnie z systemem nadzoru państwa członkowskiego oraz w stosownych przypadkach zgodnie z systemem zatwierdzania,

      — gdzie użytkownicy mogą uzyskać dostęp do określonego opisu danego państwa członkowskiego, dotyczącego sposobu korzystania z treści zaufanej listy i interpretowania jej w odniesieniu do wyszczególnionych na niej niekwalifikowanych usług zaufania lub usług zaufania określonych na szczeblu krajowym. Można to wykorzystać do wskazania potencjalnego poziomu szczegółowości krajowych systemów zatwierdzania związanych z CSP/TSP niewystawiającymi certyfikatów kwalifikowanych oraz do wskazania sposobu wykorzystania do tego celu pól »Scheme service definition URI« (klauzula 5.5.6) i »Service information extension« (klauzula 5.5.9);

   b) państwa członkowskie mogą definiować i stosować dodatkowe URI rozszerzające wskazany powyżej URI właściwy dla państwa członkowskiego (tzn. URI zdefiniowany na podstawie danego hierarchicznego określonego URI).";

3) w rozdziale II po sekcji zatytułowanej „Service current status (obecny status usługi) (klauzula 5.5.4)" dodaje się sekcję w brzmieniu:

„**The Signature element (element podpisu) (klauzula B.1), General (zasady ogólne) (klauzula B.1.0)**

Niniejsza klauzula jest obowiązkowa i musi być zgodna ze specyfikacjami zawartymi w klauzuli B.1.0 TS 119 612, gdzie pkt 2 otrzymuje brzmienie:

»2) Jego element ds:SignedInfo musi zawierać element ds:Reference z atrybutem URI ustawionym na pusty ciąg (tj. URI=""), tak aby odnosił się do całego dokumentu. Ten element ds:Reference musi spełniać następujące wymogi:

   a) musi zawierać tylko jeden element ds:Transforms;

   b) Ten element ds:Transforms musi zawierać dwa elementy ds:Transform. Pierwszym będzie ten, którego atrybut Algorithm wskazuje na transformację chronioną o wartości: "http://www.w3.org/2000/09/xmldsig#enveloped-signature". Drugim będzie ten, którego atrybut Algorithm nakazuje sprowadzenie do postaci kanonicznej zgodnie ze standardem Exclusive Canonicalization "http://www.w3.org/2001/10/xml-exc-c14n#".«".

([1]) ISO 3166-1:2006 »Kody nazw krajów i ich jednostek administracyjnych – Część 1: Kody krajów«.