

A BIZOTTSÁG (EU) 2015/1505 VÉGREHAJTÁSI HATÁROZATA**(2015. szeptember 8.)**

a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 22. cikkének (5) bekezdése szerinti bizalmi listákhoz kapcsolódó technikai specifikációk és formátumok meghatározásáról

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló, 2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendeletre ⁽¹⁾ és különösen annak 22. cikke (5) bekezdésére,

mivel:

- (1) A bizalmi listák elengedhetetlenek a piaci szereplők bizalmának megteremtéséhez, mivel e listák jelzik a szolgáltató státusát a felügyelet időpontjában.
- (2) Az elektronikus aláírások határon átnyúló használatát a Bizottság a 2009/767/EK határozattal ⁽²⁾ is előmozdította, amely kötelezően előírta a tagállamok számára, hogy hozzanak létre, tartsanak fenn és tegyenek közzé olyan bizalmi listát, amelyben szerepelnek az 1999/93/EK európai parlamenti és tanácsi irányelvvel ⁽³⁾ összhangban a nyilvánosság számára minősített tanúsítványt kiállító, a tagállamok által felügyelt és akkreditált hitelesítésszolgáltatókra vonatkozó adatok.
- (3) A 910/2014/EU rendelet 22. cikke kötelezően előírja a tagállamok számára, hogy biztonságos módon és automatizált feldolgozásra alkalmas formában hozzanak létre, tartsanak fenn és tegyenek közzé elektronikus aláírással vagy bélyegzővel ellátott bizalmi listát, és jelentsék be a Bizottságnak a nemzeti bizalmi lista létrehozásáért felelős szerveket.
- (4) Egy bizalmi szolgáltató és az általa nyújtott bizalmi szolgáltatások akkor tekintendők minősítettnek, ha a bizalmi listában minősített státus van a szolgáltatóhoz rendelve. Annak biztosítására, hogy a szolgáltatók távolból, elektronikus eszközökkel könnyen meg tudjanak felelni a 910/2014/EU rendeletből – különösen annak 27. és 37. cikkében foglaltakból – eredő egyéb kötelezettségeknek, és hogy megfeleljenek más olyan hitelesítésszolgáltatók jogos elvárásainak, amelyek nem állítanak ki minősített tanúsítványokat, de az 1999/93/EK irányelv szerint elektronikus aláírásokhoz kapcsolódó szolgáltatásokat nyújtanak és 2016. június 30-ig felkerülnek a listára, biztosítani kell a lehetőséget a tagállamok számára, hogy önkéntes alapon és nemzeti szinten a minősített szolgáltatásoktól eltérő bizalmi szolgáltatásokat is felvehessenek a bizalmi listára, feltéve, hogy világosan jelezve van, hogy ezek a szolgáltatások nincsenek a 910/2014/EU rendelet értelmében minősítve.
- (5) A 910/2014/EU rendelet (25) preambulumbekkezdésével összhangban a tagállamok a 910/2014/EU rendelet 3. cikkének 16. pontjában meghatározottaktól eltérő típusú, nemzeti szinten meghatározott bizalmi szolgáltatásokat is felvehetnek a listára, feltéve, hogy világosan jelezve van, hogy ezek a szolgáltatásokat nincsenek a 910/2014/EU rendelet értelmében minősítve.
- (6) Az e határozatban előírt intézkedések összhangban vannak a 910/2014/EU rendelet 48. cikkével létrehozott bizottság véleményével,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

A tagállamok bizalmi listát hoznak létre, tartanak fenn és tesznek közzé, amelyben szerepelnek a felügyeletük alá tartozó minősített bizalmi szolgáltatókra vonatkozó információk, valamint az e szolgáltatók által nyújtott minősített bizalmi szolgáltatásokra vonatkozó információk. E listának meg kell felelnie az I. mellékletben található technikai specifikációknak.

⁽¹⁾ HL L 257., 2014.8.28., 73. o.

⁽²⁾ A Bizottság 2009. október 16-i 2009/767/EK határozata az eljárásoknak a belső piaci szolgáltatásokról szóló 2006/123/EK európai parlamenti és tanácsi irányelv szerinti egyablakos ügyintézési pontokon keresztül elektronikus eszközökkel történő teljesítését lehetővé tevő rendelkezések meghatározásáról (HL L 274., 2009.10.20., 36. o.).

⁽³⁾ Az Európai Parlament és a Tanács 1999. december 13-i 1999/93/EK irányelve az elektronikus aláírásra vonatkozó közösségi keretfeltételekről (HL L 13., 2000.1.19., 12. o.).

2. cikk

A tagállamok a bizalmi listában szerepeltethetnek adatokat a nem minősített bizalmi szolgáltatókról és az általuk nyújtott nem minősített bizalmi szolgáltatásokról. A listában egyértelműen jelezni kell, hogy mely bizalmi szolgáltatók és mely bizalmi szolgáltatásaik nem minősítettek.

3. cikk

(1) A 910/2014/EU rendelet 22. cikkének (2) bekezdése értelmében a tagállamok az I. mellékletben megadott technikai specifikációnak megfelelően elektronikus aláírással vagy bélyegzővel látják el bizalmi listájuk automatizált feldolgozásra alkalmas változatát.

(2) Amennyiben egy tagállam a bizalmi lista emberi által olvasható változatát is elektronikusan közzéteszi, gondoskodnia kell arról, hogy a bizalmi lista ezen változata ugyanazokat az adatokat tartalmazza, mint az automatizált feldolgozásra alkalmas változat, és azt a tagállamnak elektronikus aláírással vagy bélyegzővel kell ellátnia az I. mellékletben ismertetett technikai specifikációnak megfelelően.

4. cikk

(1) A tagállamok a II. mellékletben található sablon alkalmazásával bejelentik a Bizottságnak a 910/2014/EU rendelet 22. cikkének (3) bekezdésében említett adatokat.

(2) Az (1) bekezdésben említett adatok kettő vagy több rendszerüzemeltető legalább három hónapos, elcsúsztatott érvényességi időszakokkal rendelkező nyilvános kulcsú tanúsítványát jelentik, amely kulcsok megfelelnek a bizalmi lista automatizált feldolgozásra alkalmas változatának és ember által olvasható változatának elektronikus aláírására és elektronikus bélyegzővel való ellátására felhasználható titkos kulcsoknak, amikor azokat közzéteszik.

(3) A Bizottság a 910/2014/EU rendelet 22. cikkének (4) bekezdése értelmében biztonságos csatornán keresztül egy hitelesített webszerveren, automatizált feldolgozásra alkalmas, aláírással vagy bélyegzővel ellátott formátumban elérhetővé teszi a nyilvánosság számára az (1) és (2) bekezdésben említett adatokat, ahogy azokat a tagállamok bejelentik.

(4) A Bizottság biztonságos csatornán keresztül, egy hitelesített webszerveren, ember által olvasható, aláírással vagy bélyegzővel ellátott formátumban elérhetővé teheti a nyilvánosság számára az (1) és (2) bekezdésben említett adatokat, ahogy azokat a tagállamok bejelentik.

5. cikk

Ez a határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Ez a határozat teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben, 2015. szeptember 8-án.

a Bizottság részéről
az elnök
Jean-Claude JUNCKER

I. MELLÉKLET

TECHNIKAI SPECIFIKÁCIÓK A BIZALMI LISTÁK EGYSÉGES SABLONJÁHOZ

I. FEJEZET

ÁLTALÁNOS KÖVETELMÉNYEK

A bizalmi lista tartalmazza mind a jelenlegi, mind pedig a korábbi információkat a felsorolt bizalmi szolgáltatások státusáról attól az időponttól kezdve, amikor a bizalmi szolgáltatót felvették a bizalmi listákra.

Ezen specifikációban a „jóváhagyott”, „akkreditált” és/vagy „felügyelt” kifejezések magukban foglalják a nemzeti jóváhagyási rendszereket is, de a nemzeti jóváhagyási rendszerekkel kapcsolatban a bizalmi szolgáltatók nemzeti listájában a tagállamok további információkat fognak közölni, többek között a minősített bizalmi szolgáltatókra és az általuk biztosított bizalmi szolgáltatásokra alkalmazott felügyeleti rendszerekhez viszonyított esetleges eltérésekre vonatkozóan is.

A bizalmi listában szereplő információk elsődleges célja a minősített bizalmiszolgáltatás-tokenek, azaz a bizalmi szolgáltatások igénybe vételének eredményeként generált vagy kiállított fizikai vagy bináris (logikai) objektumok, pl. a minősített elektronikus aláírások/bélyegzők, minősített tanúsítvánnyal kísért fokozott biztonságú elektronikus aláírások/bélyegzők, minősített időbélyegzők, minősített elektronikus kézbesítési igazolások stb. érvényessége ellenőrzésének támogatása.

II. FEJEZET

A BIZALMI LISTÁK EGYSÉGES SABLONJÁNAK RÉSZLETES SPECIFIKÁCIÓJA

Ez a specifikáció az ETSI TS 119 612 v2.1.1. szabványban (a továbbiakban: ETSI TS 119 612 szabvány) szereplő specifikációkon és követelményeken alapul.

Amennyiben e specifikáció külön követelményt nem tartalmaz, teljes mértékben az ETSI TS 119 612 szabvány 5. és 6. pontját kell alkalmazni. Amennyiben e specifikáció külön követelményeket tartalmaz, ezek elsőbbséget élveznek az ETSI TS 119 612 szabvány vonatkozó követelményeivel szemben. A e specifikáció és az ETSI TS 119 612 szabvány specifikációja közötti ütközés esetén ez a specifikáció az irányadó.

Scheme name (Rendszer neve) (5.3.6. pont)

Ennek a mezőnek szerepelnie kell és meg kell felelnie az ETSI TS 119 612 szabvány 5.3.6. pontjában meghatározott követelményeknek, és a rendszerre az alábbi nevet kell alkalmazni:

„EN_name_value” = „A belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályaon kívül helyezéséről szóló, 2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendeletben meghatározott releváns rendelkezések szerinti, a kiállító tagállam által felügyelt minősített bizalmi szolgáltatókkal kapcsolatos adatokat, valamint az általuk biztosított minősített bizalmi szolgáltatásokkal kapcsolatos adatokat tartalmazó bizalmi lista.”

Scheme information URI (A rendszer adatainak URI-ja) (5.3.7. pont)

Ennek a mezőnek szerepelnie kell és meg kell felelnie az ETSI TS 119 612 szabvány 5.3.7. pontjában meghatározott követelményeknek, és az „appropriate information about the scheme” (a rendszerre vonatkozó megfelelő adatok) mezőnek legalább a következőket kell tartalmaznia:

- Általános bevezető adatok, amelyek a bizalmi listák alkalmazási köre és kontextusa tekintetében valamennyi tagállam esetében azonosak, valamint az alkalmazott támogató felügyeleti, és adott esetben a nemzeti jóváhagyási (pl. akkreditációs) rendszer(ek). Az azonos szövegrész az alábbi szöveg, amelyben „[az érintett tagállam neve]” szövegrészt az érintett tagállam nevével kell helyettesíteni:

„Ez a lista az a bizalmi lista, amely a [az érintett tagállam neve] által felügyelt minősített bizalmi szolgáltatókra vonatkozó adatokat, valamint az általuk biztosított minősített bizalmi szolgáltatásokra vonatkozó adatokat tartalmaz a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályaon kívül helyezéséről szóló, 2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendeletben meghatározott vonatkozó rendelkezések szerint.

Az elektronikus aláírások határokön átnyúló használatát a 2009. október 16-i 2009/767/EK bizottsági határozat is előmozdította, amely kötelezően előírta a tagállamok számára, hogy állítsanak össze, tartsanak fenn és tegyenek közzé olyan bizalmi listát, amelyekben szerepelnek az elektronikus aláírásra vonatkozó közösségi keretfeltételekről szóló, 1999. december 13-i 1999/93/EK európai parlamenti és tanácsi irányelvvel összhangban a nyilvánosság számára minősített tanúsítványt kiállító, a tagállamok által felügyelt/akkreditált hitelesítésszolgáltatókra vonatkozó adatok. Ez a bizalmi lista a 2009/767/EK határozattal létrehozott bizalmi lista folytatása.”

A bizalmi listák elengedhetetlenek a piaci szereplők bizalmának megteremtéséhez, mivel azok alapján a felhasználók megállapíthatják a bizalmi szolgáltatóknak és azok szolgáltatásainak minősített státusát és korábbi státusait.

A tagállamok bizalmi listái legalább az (EU) 2015/1505 bizottsági végrehajtási határozat 1. és 2. cikkében meghatározott információkat tartalmaznak.

A tagállamok a bizalmi listákban szerepeltethetnek adatokat a nem minősített bizalmi szolgáltatókról és az általuk nyújtott nem minősített szolgáltatásokról. Egyértelműen jelezni kell, hogy ezek nincsenek a 910/2014/EU rendelet szerint minősítve.

A Tagállamok a bizalmi listákba felvehetnek a 910/2014/EU rendelet 3. cikkének 16. pontjában meghatározottakon kívül más típusú, nemzeti szinten meghatározott bizalmi szolgáltatásokról szóló információkat is. Egyértelműen jelezni kell, hogy ezek nincsenek a 910/2014/EU rendelet szerint minősítve.

b) Egyedi információk a támogató felügyeleti rendszerről és – adott esetben – a nemzeti jóváhagyási (pl. akkreditációs) rendszer(ek)ről, különösen ⁽¹⁾:

(1) Adatok minősített és nem minősített bizalmi szolgáltatók nemzeti felügyeleti rendszeréről és az általuk a 910/2014/EU rendelet rendelkezései szerint biztosított minősített és nem minősített bizalmi szolgáltatásokról.

(2) Adatok – adott esetben – az 1999/93/EK irányelv szerint minősített tanúsítványokat kiállító hitelesítésszolgáltatók önkéntes nemzeti akkreditációs rendszereiről.

Ezeknek a külön adatoknak a fentiekben felsorolt minden alkalmazott támogató rendszer tekintetében tartalmazniuk kell legalább a következőket:

(1) általános leírás;

(2) információk a nemzeti felügyeleti rendszer és – adott esetben – egy nemzeti jóváhagyási rendszer általi jóváhagyás esetében használt eljárásokról;

(3) információk azokról a feltételekről, amelyek alapján a bizalmi szolgáltatókat felügyelik vagy – adott esetben – jóváhagyják;

(4) információk a felügyelők/auditorok kiválasztására használt szempontokról és szabályokról, valamint annak a meghatározása, hogy hogyan értékeli a bizalmi szolgáltatókat és az általuk biztosított bizalmi szolgáltatásokat;

(5) adott esetben a rendszer üzemeltetésére vonatkozó egyéb kapcsolattartási és általános adatok.

Scheme type/community/rules (Rendszertípus, közösség, szabályok) (5.3.9. pont)

Ennek a mezőnek szerepelnie kell és meg kell felelnie az ETSI TS 119 612 szabvány 5.3.9. pontjában meghatározott követelményeknek.

Csak brit angol URI-kat tartalmazhat.

⁽¹⁾ Ezek az adatcsoportok kulcsfontosságúak a listát igénybe vevő felek számára az ilyen rendszerek minőségének és biztonsági szintjének értékeléséhez. Ezeket az adatcsoportokat a bizalmi lista szintjén kell megadni, „a rendszer adatainak URI-ja” (Scheme information URI) (5.3.7. pont – tagállamok által megadott adatok), a „rendszertípus/közösség/szabályok” (Scheme type/community/rules) (5.3.9. pont – valamennyi tagállam esetében azonos szöveggel) és a „megbízhatósági állapotlista szabályzat/jogi nyilatkozat” (TSL policy/legal notice) (5.3.11. pont – valamennyi tagállam esetében azonos szöveg, azzal, hogy minden tagállam feltüntetheti a tagállamra jellemző egyedi szöveget/hivatkozásokat) mezők használatával. A nem minősített bizalmi szolgáltatások és nemzeti szinten meghatározott (minősített) bizalmi szolgáltatások ilyen rendszereiről további adatokat szükség esetén (pl. több minőségi/biztonsági szint megkülönböztetése érdekében) szolgáltatási szinten lehet megadni „a rendszer szolgáltatásai meghatározásának URI-ja” (Scheme service definition URI) (5.5.6. pont) mező használatával.

Legalább a következő két URI-t tartalmazza:

- (1) A bizalmi szolgáltatók valamennyi tagállami listája tekintetében azonos URI, amely olyan leíró szövegre mutat, amelynek a bizalmi szolgáltatók összes listájára vonatkozik, az alábbiak szerint:

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

Leíró szöveg:

„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 provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

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.

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 that they provide meet the requirements laid down in the Regulation.

The trusted lists of Member States include, as a minimum, information specified in Articles 1 and 2 of Commission 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 (e.g. accreditation) scheme(s) under which the trust service providers and the trust services that they provide are listed.

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:

The »qualified« status of a trust service is indicated by the combination of the »Service type identifier« (»Sti«) value in a service entry 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.

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 (possibly further qualified as being a »RootCA-QC« through the use of the appropriate »Service information extension« (»Sie«) additionalServiceInformation Extension)

— indicates that any end-entity certificate issued by or under the CA represented by the »Service digital identifier« (»Sdi«) CA's public key and CA's name (both CA data to be considered as trust anchor input), is a qualified certificate (QC) provided that it includes at least one of the following:

- the id-etsi-qcs-QcCompliance ETSI defined statement (id-etsi-qcs 1),
- the 0.4.0.1456.1.1. (QCP+) ETSI defined certificate policy OID,

— the 0.4.0.1456.1.2. (QCP) ETSI defined certificate policy OID,

and provided this is ensured by the Member State Supervisory Body through a valid service status (i.e. »undersupervision«, »supervisionincessation«, »accredited« or »granted«) for that entry,

— and IF »Sie« »Qualifications Extension« information is present, then in addition to the above default rule, those certificates that are identified through the use of »Sie« »Qualifications Extension« information, constructed as a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing additional information regarding their qualified status, the »SSCD support« and/or »Legal person as subject« (e.g. certificates containing a specific OID in the Certificate Policy extension, and/or having a specific »Key usage« pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, etc.). These qualifiers are part of the following set of »Qualifiers« used to compensate for the lack of information in the corresponding certificate content, and that are used respectively:

— to indicate the qualified certificate nature:

— »QCStatement« meaning the identified certificate(s) is(are) qualified under Directive 1999/93/EC,

— »QCForESig« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic signature under Regulation 910/2014/EU,

— »QCForESeal« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic seal under Regulation 910/2014/EU,

— »QCForWSA« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for web site authentication under Regulation 910/2014/EU,

— to indicate that the certificate is not to be considered as qualified:

— »NotQualified« meaning the identified certificate(s) is(are) not to be considered as qualified, and/or

— to indicate the nature of the SSCD support:

— »QCWithSSCD« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in an SSCD, or

— »QCNoSSCD« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in an SSCD, or

— »QCSSCDStatusAsInCert« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key residing in an SSCD,

— to indicate the nature of the QSCD support:

— »QCWithQSCD« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in a QSCD, or

— »QCNoQSCD« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in a QSCD, or

— »QCQSCDStatusAsInCert« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key is residing in a QSCD,

— »QCQSCDManagedOnBehalf« indicating that all certificates identified by the applicable list of criteria, 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, and/or

— to indicate issuance to Legal Person:

- »QCForLegalPerson« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), 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:

- if none of the id-etsi-qcs 1 statement, QCP OID or QCP+ OID information is included in an end-entity certificate, 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,

then the certificate is not to be considered as qualified.

»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 TL information, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing 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.

The general rule for interpretation of any other »Sti« type entry is that, for that »Sti« identified service type, the listed service named according to the »Service name« field value and uniquely identified by the »Service digital identity« field value has the current qualified or 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 applicable secondary legislation pursuant to Regulation (EU) No 910/2014 for further details on the fields, description and meaning for the Member States' trusted lists."

- (2) Az egyes tagállamok bizalmi listáinak egyedi URI-ja, amely az adott tagállam bizalmi listájára alkalmazandó leíró szövegre mutat:

<http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC>, ahol CC = a „Scheme territory” (a rendszer területi hatálya) mezőben (5.3.10. pont) használt ISO 3166-1 ⁽¹⁾ alpha-2 országkód

- Ahol a felhasználók elérhetik az adott tagállam azon egyedi szabályzatát/szabályait, amelyek alapján a listán szereplő szolgáltatásokat értékelik a tagállam felügyeleti rendszerének és – adott esetben – jóváhagyási rendszerének megfelelően.
- Ahol a felhasználók elérhetik az adott tagállamra vonatkozó külön leírásokat arról, hogy miként kell a bizalmi lista tartalmát értelmezni a listán szereplő nem minősített bizalmi szolgáltatásokkal és/vagy nemzeti szinten meghatározott bizalmi szolgáltatásokkal kapcsolatban. Ezzel jelezni lehet a minősített tanúsítványok kiadásával nem foglalkozó hitelesítésszolgáltatók nemzeti jóváhagyási rendszerének potenciális granularitását és azt, hogy a „Scheme service definition URI” (a rendszer szolgáltatásai meghatározásának URI-ja) (5.5.6. pont) és a „Service information extension” (szolgáltatásadat-bővítmény) (5.5.9. pont) mezőket miként használják erre a célra.

A tagállamoknak LEHETŐSÉGÜK VAN a fenti tagállam-specifikus URI-t kibővítő további URI-ket (azaz ebből a hierarchikus specifikus URI-ből meghatározott URI-ket) meghatározni és használni.

TSL policy/legal notice (megbízhatósági állapotlista szabályzat/jogi nyilatkozat) (5.3.11. pont)

Ennek a mezőnek szerepelnie kell és meg kell felelnie az ETSI TS 119 612 szabvány 5.3.11. pontjában meghatározott követelményeknek, amelyek szerint a rendszer létrehozási helyének megfelelő joghatóság szerint a rendszer jogi státusára vagy a rendszer által teljesített jogi előírásokra vonatkozó szabályzatnak/jogi nyilatkozatnak és/vagy bármely

⁽¹⁾ ISO 3166-1:2006 „Országok és igazgatási egységeik nevének kódjai – 1. rész: Országkódok”.

korlátozásnak vagy feltételnek, amely alapján a bizalmi listát fenntartják és közzéteszik, egy sor többnyelvű karakterláncból kell állnia (lásd 5.1.4 pont), amelyek kötelező nyelvként brit angol nyelven és esetlegesen egy vagy több nemzeti nyelven az ilyen szabályzat vagy nyilatkozat alábbiak szerint felépített konkrét szövegét tartalmazzák:

- (1) Kötelező első rész, amely minden tagállam bizalmi listájában feltüntetendő és hivatkozik az alkalmazandó jogi keretekre, és amelynek angol nyelvű változata a következő:

The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

A közös szöveg magyar nyelvű változata:

E bizalmi lista alkalmazandó jogi kerete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló, 2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendelet.

- (2) Második, választható, az egyes bizalmi listákra jellemző rész, amely a meghatározott alkalmazandó nemzeti jogi keretekre való hivatkozásokat tartalmaz

Service current status (Szolgáltatás aktuális státusa) (5.5.4. pont)

Ennek a mezőnek szerepelnie kell és meg kell felelnie az ETSI TS 119 612 szabvány 5.5.4. pontjában meghatározott követelményeknek.

Az EUMS bizalmi listában a 910/2014/EU rendelet alkalmazását megelőző naptól (azaz 2016. június 30-tól) felsorolt szolgáltatások „Service current status” értékének migrációját az ETSI TS 119 612 J. mellékletének előírásai szerint a rendelet alkalmazásának napján (azaz 2016. július 1-jén) kell végrehajtani.

III. FEJEZET

A BIZALMI LISTÁK FOLYTONOSSÁGA

A tanúsítványoknak, amelyeket e határozat 4. cikkének (2) bekezdése szerint a Bizottságnak jelenteni kell, meg kell felelniük az ETSI TS 119 612 5.7.1. pontja követelményeinek, és azokat úgy kell kiállítani, hogy:

- érvényességük utolsó napja („Not After”) között legalább három hónap különbség legyen,
- új kulcspárok alapján készüljenek. A korábban használt kulcspárokat nem szabad újra tanúsítani.

Ha az egyik nyilvánoskulcs-tanúsítványnak, amellyel a bizalmi lista Bizottságnak bejelentett és a Bizottság által a hivatkozásokról vezetett központi listában közzétett aláírását vagy bélyegzőjét hitelesíteni lehetne, lejár az érvényessége, akkor a tagállamoknak a következőket kell tenniük:

- amennyiben a közzétett jelenlegi bizalmi listát olyan titkos kulccsal írták alá és bélyegezték le, amelynek nyilvánoskulcs-tanúsítványa lejárt, akkor késedelem nélkül egy új bizalmi listát adnak ki és azt olyan titkos kulccsal írják alá vagy bélyegzik le, amelynek a nyilvánoskulcs-tanúsítványa még nem járt le,
- szükség szerint új kulcspárokat generálnak, amelyekkel a bizalmi lista aláírható vagy lebélyegezhető, és elvégzik a hozzájuk tartozó nyilvánoskulcs-tanúsítványok generálását,
- azonnal tájékoztatják a Bizottságot a bizalmi lista aláírására vagy lebélyegzésére használható titkos kulcsokhoz tartozó nyilvánoskulcs-tanúsítványok új listájáról.

A bizalmi lista aláírásának vagy bélyegzőjének hitelesítésére felhasználható nyilvánoskulcs-tanúsítványok egyikéhez tartozó, a Bizottságnak bejelentett és a Bizottság által a hivatkozásokról vezetett központi listán közzétett titkos kulcsok egyikének veszélyeztetése vagy visszavonása esetén a tagállamok:

- haladéktalanul újból kiállítják az új, nem veszélyeztetett titkos kulccsal aláírt vagy lebélyegzett bizalmi listát, amennyiben a közzétett listát veszélyeztetett vagy visszavont titkos kulccsal írták alá vagy bélyegezték le,

- szükség szerint új kulcspárokat generálnak, amelyekkel a bizalmi lista aláírható vagy lebélyegezhető, és elvégzik a hozzájuk tartozó nyilvánoskulcs-tanúsítványok generálását,
- azonnal tájékoztatják a Bizottságot a bizalmi lista aláírására vagy lebélyegzésére használható titkos kulcsokhoz tartozó nyilvánoskulcs-tanúsítványok új listájáról.

A bizalmi lista aláírásának hitelesítésére felhasználható nyilvánoskulcs-tanúsítványokhoz tartozó, a Bizottságnak bejelentett és a Bizottság által a hivatkozásokról vezetett központi listán közzétett titkos kulcsok mindegyikének veszélyeztetése vagy visszavonása esetén a tagállamok:

- új kulcspárokat generálnak, amelyekkel a bizalmi lista aláírható vagy lebélyegezhető, és elvégzik a hozzájuk tartozó nyilvánoskulcs-tanúsítványok generálását,
- haladéktalanul újból kiállítják az új bizalmi listát, amelyet az új titkos kulcsok egyikével írnak alá vagy bélyegeznek le, és bejelentik az ahhoz tartozó nyilvánoskulcs-tanúsítványt,
- azonnal tájékoztatják a Bizottságot a bizalmi lista aláírására vagy lebélyegzésére használható titkos kulcsokhoz tartozó nyilvánoskulcs-tanúsítványok új listájáról.

IV. FEJEZET

A BIZALMI LISTA EMBER ÁLTAL OLVASHATÓ VÁLTOZATÁNAK SPECIFIKÁCIÓJA

Amennyiben létrehozzák és közzéteszik a bizalmi lista ember által olvasható változatát, azt az ISO 32000 szabványnak ⁽¹⁾ megfelelő Portable Document Format (PDF) dokumentum formájában kell elkészíteni, és annak formátumát a PDF/A (ISO 19005 ⁽²⁾) profilnak megfelelően kell kialakítani.

A bizalmi szolgáltatók listája PDF/A-alapú, ember által olvasható változatának a következő követelményeknek kell megfelelnie:

- Az ember által olvasható változat felépítésének a TS 119 612 szabványban leírt logikai modellt kell tükröznie.
- Minden megadott mezőt fel kell tüntetni, és a következőket kell megadni:
 - a mező címe (pl. „Service type identifier”),
 - a mező értéke (pl. „<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>”),
 - adott esetben a mező értékének jelentése (leírása) (pl. „A vonatkozó regisztrációs szolgáltatások által ellenőrzött személyazonosság és más jellemzők alapján minősített tanúsítványokat létrehozó és aláíró tanúsítványgeneráló szolgáltatás.”),
 - adott esetben több természetes nyelvi változat, a bizalmi listában előírtak szerint.
- A digitális tanúsítványoknak ⁽³⁾ legalább a „Service digital identity” (szolgáltatás digitális azonosítója) mezőben szereplő következő mezőit és megfelelő értékeit kell ember által olvasható formában megjeleníteni:
 - Verzió (Version)
 - Tanúsítvány sorszáma (Certificate serial number)
 - Aláíró algoritmus (Signature algorithm)
 - Kiállító (Issuer) – minden releváns, megkülönböztetésre alkalmas „név” mező
 - Érvényességi időszak (Validity period)
 - Tulajdonos (Subject) – minden releváns, megkülönböztetésre alkalmas „név” mező

⁽¹⁾ ISO 32000-1:2008 Dokumentumkezelés – Portable document format – 1. rész: PDF 1.7

⁽²⁾ ISO 19005-2:2011 Dokumentumkezelés – Elektronikus dokumentum fájlformátuma hosszú távú megőrzésre – 2. rész: Az ISO 32000-1 (PDF/A-2) szabvány használata.

⁽³⁾ ITU-T X.509 | ISO/IEC 9594-8 ajánlás: Informatika. Nyílt rendszerek összekapcsolása. Névtár: A nyilvánoskulcs- és az attribútumtanúsítvány keretszabályai (lásd <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509>).

- Nyilvános kulcs (Public key)
 - CA kulcsazonosítója (Authority Key Identifier)
 - Tulajdonos kulcsazonosítója (Subject Key Identifier)
 - Kulcshasználat (Key Usage)
 - Kibővített kulcshasználat (Extended key usage)
 - Hitelesítési rend (Certificate Policies) – minden hitelesítésirend-azonosító és hitelesítésirend-minősítő
 - Hitelesítési rend leképezései (Policy mappings)
 - Tulajdonos alternatív neve (Subject alternative name)
 - Tulajdonosnévtár-jellemzők (Subject directory attributes)
 - Alapvető típusmegkötések (Basic constraints)
 - Hitelesítésirend-megkötések (Policy constraints)
 - A tanúsítvány-visszavonási lista terjesztési helyei (CRL Distribution Points) ⁽¹⁾
 - Hozzáférés tanúsítványkiadó adataihoz
 - Hozzáférés tulajdonos adataihoz
 - Minősített-tanúsítvány-nyilatkozatok ⁽²⁾
 - Hash algoritmus
 - A tanúsítvány hash értéke
- Az ember által olvasható változatot könnyen nyomtatható formátumban kell elkészíteni.
- Az ember által olvasható változatot a rendszer üzemeltetője az (EU) 2015/1505 bizottsági végrehajtási határozat 1. és 3. cikkében meghatározott fokozott biztonságú PDF aláírás szerint aláírja és lebélyegzi.
-

⁽¹⁾ RFC 5280: Internet X.509 PKI-tanúsítvány és CRL-profil

⁽²⁾ RFC 3739: Internet X.509 PKI: Minősített tanúsítványok profilja

II. MELLÉKLET

SABLON A TAGÁLLAMI BEJELENTÉSEKHEZ

Az e határozat 4. cikkének (1) bekezdése szerint a tagállamok által bejelentendő információknak az alábbi adatokra és változásaikra kell kiterjedniük:

1. A tagállam az ISO 3166-1 ⁽¹⁾ alfa-2 kódok alkalmazásával, kivéve hogy:
 - a) az Egyesült Királyság esetében az országkód „UK”;
 - b) Görögország esetében az országkód „EL”.
2. a bizalmi listák automatizált feldolgozásra alkalmas és emberi szemmel olvasható változatának létrehozásáért, fenntartásáért és közzétételéért felelős szerv/szervek neve:
 - a) A rendszerüzemeltető neve: a megadott információknak – a kis- és nagybetűket is figyelembe véve – a bizalmi listában használt valamennyi nyelven meg kell egyeznie a bizalmi listában a „Scheme operator name” (Rendszerüzemeltető neve) értékhez rendelt megnevezéssel.
 - b) Opcionális információk a Bizottság belső használatára kizárólag olyan esetekben, ha érintkezésbe kell lépni az illetékes szervvel (ez az információ nem kerül közzétételre az Európai Bizottság által összeállított bizalmi listákban):
 - a rendszerüzemeltető címe;
 - a felelős személy(ek) elérhetőségei (név, telefon, e-mail cím).
3. A bizalmi lista automatizált feldolgozásra alkalmas változatának közzétételi helye *(az aktuális bizalmi lista közzétételi helye)*.
4. Adott esetben az ember által olvasható bizalmi lista közzétételi helye *(az aktuális bizalmi lista közzétételi helye)*. Amennyiben már nincs közzétéve ember által olvasható bizalmi lista, ennek jelzése.
5. Azok a nyilvános kulcsú tanúsítványok, amelyek megfelelnek azoknak a privát kulcsoknak, amelyekkel elektronikusan aláírható vagy lebélyegezhető a bizalmi lista automatizált feldolgozásra alkalmas változata és ember által olvasható változata: az ilyen tanúsítványokat megnövelt személyiségi jogokat biztosító levél (PEM) formátumú, base64 kódolású DER tanúsítványokként kell biztosítani. Változásbejelentés céljára további információk, ha egy új tanúsítványnak kell a Bizottság listájában szereplő konkrét tanúsítvány helyére lépnie, és ha a bejelentett tanúsítványt helyettesítés nélkül kell felvenni a meglévőbe vagy meglévőkbe
6. Az (1)–(5) pontokban bejelentett adatok benyújtásának időpontja.

Az (1), (2a), (3), (4) és (5) pont szerint bejelentett adatokat fel kell venni a bizalmi listák Európai Bizottság által összeállított listájába, az összeállított listába felvett, korábban bejelentett információk helyébe.

⁽¹⁾ ISO 3166-1 „Országok és igazgatási egységeik nevének kódjai – 1. rész: Országkódok”.