Az Európai Unió
Hivatalos Lapja

L 235

58. évfolyam

Magyar nyelvű kiadás **Jogszabályok**

2015. szeptember 9.

Tartalom

[1] EGT-vonatkozású szöveg

HU

Azok a jogi aktusok, amelyek címe normál szedéssel jelenik meg, a mezőgazdasági ügyek napi intézésére vonatkoznak, és rendszerint csak korlátozott ideig maradnak hatályban.

Valamennyi más jogszabály címét vastagon szedik, és előtte csillag szerepel.

[1] EGT-vonatkozású szöveg

II

(Nem jogalkotási aktusok)

RENDELETEK

A BIZOTTSÁG (EU) 2015/1501 VÉGREHAJTÁSI RENDELETE

(2015. szeptember 8.)

a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 12. cikkének (8) bekezdése szerinti átjárhatósági keretről

(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 12. cikke (8) bekezdésére,

mivel:

(1) A 910/2014/EU rendelet 12. cikkének (2) bekezdése alapján az ugyanazon rendelet 9. cikkének (1) bekezdése szerint bejelentett nemzeti elektronikus azonosítási rendszerek átjárhatósága céljából átjárhatósági keretet kell létrehozni.

(2) A csomópontok központi szerepet játszanak a tagállamok elektronikus azonosítási rendszereinek összekapcsolásában. Hozzájárulásuk, ezen belül az „eIDAS" csomópont funkcióinak és komponenseinek magyarázata az 1316/2013/EU európai parlamenti és tanácsi rendelet ([2]) által létrehozott Európai Hálózatfinanszírozási Eszközzel kapcsolatos dokumentációban található.

(3) Ha egy tagállam vagy a Bizottság olyan szoftvert biztosít, amely lehetővé teszi a hitelesítést egy másik tagállamban üzemeltetett csomópontnál, a hitelesítési mechanizmushoz használt szoftvert szállító és frissítő fél megállapodhat a szoftvert üzemeltető féllel a hitelesítési mechanizmus üzemelésének irányításáról. Az ilyen megállapodások nem támaszthatnak aránytalan technikai követelményeket vagy költségeket (ezen belül támogatást, felelősségvállalást, üzemeltetési és egyéb költségeket) az üzemeltető fél számára.

(4) Amennyire azt az átjárhatósági keret megvalósítása indokolja, a Bizottság az e rendeletben megadott technikai követelményeket részletező további technikai specifikációkat dolgozhat ki a tagállamokkal együttműködésben, figyelembe véve különösen a 2015/296/EU ([3]) bizottsági végrehajtási határozat 14. cikkének d) pontjában említett együttműködési hálózat által kiadott szakvéleményeket. Az ilyen specifikációkat az 1316/2013/EU rendelet szerinti digitális szolgáltatási infrastruktúrák részeként kell kidolgozni, amely rendelet biztosítja az eszközt egy elektronikus azonosítást szolgáló rendszerelem gyakorlati megvalósításához.

([1]) HL L 257., 2014.8.28., 73. o.

([2]) Az Európai Parlament és a Tanács 2013. december 11-i 1316/2013/EU rendelete az Európai Hálózatfinanszírozási Eszköz létrehozásáról, a 913/2010/EU rendelet módosításáról és a 680/2007/EK és 67/2010/EK rendelet hatályon kívül helyezéséről (HL L 348., 2013.12.20., 129. o.).

([3]) A Bizottság 2015. február 24-i (EU) 2015/296 végrehajtási határozata a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 12. cikkének (7) bekezdése értelmében vett, a tagállamok által az elektronikus azonosítás területén folytatandó együttműködésre vonatkozó eljárási szabályok megállapításáról (HL L 53., 2015.2.25., 14. o.)

(5) Az e rendeletben megállapított technikai követelményeknek a rendelet 12. cikke alapján esetlegesen kidolgozott technikai specifikációkban történő bármely változás ellenére alkalmazhatónak kell lenniük.

(6) Az e rendeletben megállapított átjárhatósági keretre vonatkozó szabályok kialakításakor a lehető legnagyobb mértékben figyelembe vettük a nagyszabású STORK kísérleti projektet, és ezen belül a projekt keretében kidolgozott előírásokat, valamint az európai közszolgáltatásokra vonatkozó európai átjárhatósági keret elveit és fogalmait.

(7) A tagállamok közötti együttműködés eredményeit a legmesszebbmenőkig figyelembe vettük.

(8) Az e rendeletben előírt intézkedések összhangban vannak a 910/2014/EU rendelet 48. cikkével létrehozott bizottság véleményével,

ELFOGADTA EZT A RENDELETET:

1. cikk

A rendelet tárgya

Ez a rendelet az átjárhatósági keret technikai és üzemeltetési követelményeit állapítja meg annak érdekében, hogy biztosítsa a tagállamok által a Bizottságnak bejelentett elektronikus azonosítási rendszerek átjárhatóságát.

E követelmények magukban foglalják különösen a következőket:

a) a biztonsági szintekhez tartozó minimális technikai követelmények és a bejelentett elektronikus azonosítási rendszer keretében kibocsátott bejelentett elektronikus azonosítási eszközök 910/2014/EU rendelet 8. cikke szerinti nemzeti biztonsági szintjeinek megfeleltetése, ahogy azok a 3. és 4. cikkben szerepelnek;

b) az átjárhatóság minimális technikai követelményei, ahogy azok az 5. és 8. cikkben szerepelnek;

c) az egy természetes vagy jogi személyt kizárólagosan azonosító minimális személyazonosító adatok, ahogy azok a 11. cikkben és a mellékletben szerepelnek;

d) közös üzembiztonsági normák, ahogy azok a 6., 7., 9. és 10. cikkben szerepelnek;

e) vitarendezési eljárások, ahogy azok a 13. cikkben szerepelnek.

2. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

1. „csomópont”: olyan kapcsolódási pont, amely az elektronikus azonosítási átjárhatósági architektúra része, részt vesz személyek határokon átnyúló hitelesítésében, és amely képes adatátvitel felismerésére és feldolgozására vagy más csomópontokhoz történő továbbítására oly módon, hogy képessé teszi egy tagállam nemzeti elektronikus azonosítási infrastruktúráját arra, hogy interfészen keresztül kapcsolódjon más tagállamok nemzeti elektronikus azonosítási infrastruktúrájához;

2. „csomópont-üzemeltető”: olyan szervezet, amely azért felel, hogy a csomópont kapcsolódási pontként megfelelően és megbízhatóan ellássa funkcióit.

3. cikk

A biztonsági szintekhez kapcsolódó minimális technikai követelmények

A biztonsági szintekhez kapcsolódó minimális technikai követelmények az (EU) 2015/1502 bizottsági végrehajtási rendeletben ([1]) megállapított követelmények.

4. cikk

A nemzeti biztonsági szintek megfeleltetése

A bejelentett elektronikus azonosítási rendszerek nemzeti biztonsági szintjeinek megfeleltetése az (EU) 2015/1502 bizottsági végrehajtási rendeletben megállapított követelmények szerint történik. A megfeleltetés eredményeit az (EU) 2015/1505 bizottsági végrehajtási határozatban ([2]) előírt bejelentési formanyomtatvány alkalmazásával be kell jelenteni a Bizottságnak.

5. cikk

Csomópontok

(1) A tagállamok csomópontjainak össze kell tudniuk kapcsolódni más tagállamok csomópontjaival.

(2) A csomópontoknak technikai eszközök révén meg kell tudniuk különböztetni a közigazgatási szerveket és a magánszektorbeli igénybevevő feleket.

(3) Az e rendeletben megállapított technikai követelmények egyik tagállam általi megvalósítása nem járhat aránytalan technikai követelményekkel és költségekkel más tagállamok számára az első tagállamban megvalósított rendszerrel való együttműködés érdekében.

6. cikk

Adatvédelem és titoktartás

(1) A kicserélt adatok titkosságának és bizalmas jellegének védelmét és az adatok sértetlenségének fenntartását a csomópontok között a legjobb rendelkezésre álló technikai megoldások és védelmi gyakorlatok alkalmazásával kell biztosítani.

(2) A csomópontok a 9. cikk (3) bekezdésében megadott célokra használt adatok kivételével semmilyen személyes adatot nem tárolhatnak.

7. cikk

A továbbított adatok sértetlensége és hitelessége

A csomópontok közötti kommunikációnak biztosítania kell az adatok sértetlenségét és hitelességét annak biztosítása érdekében, hogy minden kérés és válasz autentikus, és nem manipulálták őket. E célra a csomópontoknál olyan megoldásokat kell alkalmazni, amelyet sikeresen alkalmaztak határokon átnyúló üzemi használatban.

([1]) A Bizottság 2015. szeptember 8-i (EU) 2015/1502 végrehajtási rendelete az elektronikus azonosító eszközök biztonsági szintjeire vonatkozó minimális technikai specifikációknak és eljárásoknak a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 8. cikkének (3) bekezdése szerint történő megállapításáról (lásd e Hivatalos Lap 7. oldalát).

([2]) A Bizottság 2015. szeptember 8-i (EU) 2015/1505 végrehajtási határozata 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 (lásd e Hivatalos Lap 26. oldalát).

8. cikk

Az átvitel üzenetformátuma

A csomópontoknál szintaxisként olyan normákon alapuló általános üzenetformátumokat kell alkalmazni, amelyeket a tagállamok között többször is alkalmaztak, és amelyek üzemi körülmények között működőképesnek bizonyultak. A szintaxisnak lehetővé kell tenni a következőket:

a) egy természetes vagy jogi személyt kizárólagosan azonosító minimális személyazonosító adatok megfelelő feldolgozása;

b) az elektronikus azonosító eszköz biztonsági szintjének megfelelő feldolgozása;

c) a közigazgatási szervek és más igénybevevő felek megkülönböztetése;

d) rugalmasság az azonosításhoz kapcsolódó további attribútumok igényeinek kielégítéséhez.

9. cikk

A biztonsági információk és a metaadatok kezelése

(1) A csomópont-üzemeltetőnek a csomópont-irányítás metaadatait szabványosított, gépileg feldolgozható, illetve biztonságos és megbízható módon kell továbbítania.

(2) Legalább a biztonság szempontjából releváns paramétereket automatikusan kell lehívni.

(3) A csomópont-üzemeltetőnek tárolnia kell azokat az adatokat, amelyek biztonsági esemény esetén lehetővé teszik az üzenetcsere szekvenciájának rekonstruálását az esemény helyének és jellegének megállapításához. Az adatokat a nemzeti követelményekben megállapított időtartamig kell tárolni, és minimálisan a következő elemekből kell állniuk:

a) a csomópont azonosítása;

b) az üzenet azonosítása;

c) az üzenet napja és időpontja.

10. cikk

Információvédelem és biztonsági normák

(1) A hitelesítést biztosító csomópontok csomópont-üzemeltetőinek tanúsítás, vagy ezzel egyenértékű vizsgálati módszerek, vagy a nemzeti jogszabályoknak való megfelelés révén igazolniuk kell, hogy az átjárhatósági keretbe tartozó csomópontok tekintetében a csomópont teljesíti az ISO/IEC 27001 szabvány követelményeit.

(2) A csomópont-üzemeltetőknek indokolatlan késedelem nélkül alkalmazniuk kell a kritikus biztonsági frissítéseket.

11. cikk

Személyazonosító adatok

(1) Határokon átnyúló esetekben az egy természetes vagy jogi személyt kizárólagosan azonosító minimális személyazonosító adatoknak teljesíteniük kell a mellékletben megállapított követelményeket.

(2) Határokon átnyúló esetekben az egy jogi személyt képviselő természetes személynél a minimális adatoknak a mellékletben a természetes és jogi személyekre felsorolt attribútumok kombinációját kell tartalmazniuk.

(3) Az adatokat az eredeti karakterek alapján kell továbbítani, és szükség esetén latin betűs átírást kell alkalmazni.

12. cikk

Technikai specifikációk

(1) Ahol azt az átjárhatósági keret megvalósítási folyamata indokolja, az (EU) 2015/296 bizottsági végrehajtási határozat alapján létrehozott együttműködési hálózat ugyanazon határozat 14. cikkének d) pontjával összhangban szakvéleményeket fogadhat el technikai specifikációk kidolgozásának szükségességéről. Az ilyen technikai specifikációk tovább részletezik az e rendeletben megállapított technikai követelményeket.

(2) Az (1) bekezdésben említett szakvélemények alapján a Bizottság a tagállamokkal együttműködésben az 1316/2013/EU rendelet szerinti digitális szolgáltatási infrastruktúra részeként kidolgozza a technikai specifikációkat.

(3) Az együttműködési hálózatnak el kell fogadnia egy, az (EU) 2015/296 bizottsági végrehajtási határozat 14. cikkének d) pontja szerinti szakvéleményt, amelyben értékeli, hogy a (2) bekezdés alapján kidolgozott technikai specifikációk megfelelnek-e, és ha igen, milyen mértékben felelnek meg az (1) bekezdésben említett szakvéleményben megállapított szükségletnek vagy az e rendeletben megállapított követelményeknek. Javasolhatja, hogy a tagállamok az átjárhatósági keret megvalósításakor vegyék figyelembe a technikai specifikációkat.

(4) A Bizottságnak a technikai specifikációk értelmezéséhez példaként referenciaalkalmazást kell megadnia. A tagállamok alkalmazhatják ezt a referenciaalkalmazást vagy mintaként használhatják a technikai specifikációk más megvalósításainak tesztelésekor.

13. cikk

Vitarendezés

(1) Amennyiben lehetséges, az átjárhatósági keretet érintő vitákat az érintett tagállamoknak tárgyalás útján kell rendezniük.

(2) Amennyiben nem sikerül az (1) bekezdéssel összhangban megoldásra jutni, a vitában az (EU) 2015/296 végrehajtási határozat 12. cikke alapján létrehozott együttműködési hálózat – saját eljárásrendje szerint – illetékes.

14. cikk

Hatálybalépés

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

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

Kelt Brüsszelben, 2015. szeptember 8-án.

a Bizottság részéről

az elnök

Jean-Claude JUNCKER

MELLÉKLET

Az egy természetes vagy jogi személyt kizárólagosan azonosító minimális személyazonosító adatokra vonatkozó, a 11. cikkben említett követelmények

1. **Minimálisan megadandó adatok természetes személyek esetén**

Természetes személyek esetén a minimálisan megadandó adatoknak az alábbi kötelező attribútumok mindegyikét tartalmazniuk kell:

a) aktuális vezetéknév/vezetéknevek;

b) aktuális keresztnév/keresztnevek;

c) születési idő;

d) a küldő tagállam által a technikai specifikációkkal összhangban, a határokon átnyúló azonosítás céljára létrehozott egyedi azonosító, amely időben a lehető legtartósabb.

Természetes személyek esetén a minimálisan megadandó adatok az alábbi kiegészítő attribútumok közül egyet vagy többet is tartalmazhatnak:

a) születéskori keresztnév/keresztnevek és vezetéknév/vezetéknevek;

b) születési hely;

c) aktuális lakcím;

d) nem.

2. **Minimálisan megadandó adatok jogi személyek esetén**

Jogi személyek esetén a minimálisan megadandó adatoknak az alábbi kötelező attribútumok mindegyikét tartalmazniuk kell:

a) aktuális jogi elnevezés;

b) a küldő tagállam által a technikai specifikációkkal összhangban, a határokon átnyúló azonosítás céljára létrehozott egyedi azonosító, amely időben a lehető legtartósabb.

Jogi személyek esetén a minimálisan megadandó adatok az alábbi kiegészítő attribútumok közül egyet vagy többet is tartalmazhatnak:

a) aktuális cím;

b) héaazonosító szám;

c) adónyilvántartási szám;

d) a 2009/101/EK európai parlamenti és tanácsi irányelv ([1]) 3. cikkének (1) bekezdéséhez kapcsolódó azonosító;

e) az 1247/2012/EU bizottsági végrehajtási rendeletben ([2]) említett jogalany-azonosító (LEI);

f) az 1352/2013/EU bizottsági végrehajtási rendeletben ([3]) említett EORI-szám (gazdasági szereplők nyilvántartása és azonosítása);

g) a 389/2012/EU bizottsági rendelet ([4]) 2. cikkének 12. pontja szerinti jövedéki szám.

([1]) Az Európai Parlament és a Tanács 2009. szeptember 16-i 2009/101/EK irányelve az egész Közösségre kiterjedő egységes biztosítékok kialakítása érdekében a tagállamok által a társasági tagok és harmadik személyek érdekei védelmében a Szerződés 48. cikkének második bekezdése szerinti társaságoknak előírt biztosítékok összehangolásáról (HL L 258., 2009.10.1., 11. o.).

([2]) A Bizottság 2012. december 19-i 1247/2012/EU végrehajtási rendelete a tőzsdén kívüli származtatott ügyletekről, a központi szerződő felekről és a kereskedési adattárakról szóló 648/2012/EU európai parlamenti és tanácsi rendeletnek megfelelően a kereskedési adattáraknak benyújtandó kereskedési jelentések formátumára és gyakoriságára vonatkozó végrehajtási technikai standardok meghatározásáról (HL L 352., 2012.12.21., 20. o.)

([3]) A Bizottság 2013. december 4-i 1352/2013/EU végrehajtási rendelete a szellemi tulajdonjogok vámhatósági érvényesítéséről szóló 608/2013/EU európai parlamenti és tanácsi rendeletben meghatározott formanyomtatványok kidolgozásáról (HL L 341., 2013.12.18., 10. o.)

([4]) A Tanács 2012. május 2-i 389/2012/EU rendelete a jövedéki adók területén való közigazgatási együttműködésről és a 2073/2004/EK rendelet hatályon kívül helyezéséről (HL L 121., 2012.5.8., 1. o.).

A BIZOTTSÁG (EU) 2015/1502 VÉGREHAJTÁSI RENDELETE

(2015. szeptember 8.)

az elektronikus azonosító eszközök biztonsági szintjeire vonatkozó minimális technikai specifikációknak és eljárásoknak a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 8. cikkének (3) bekezdése szerint történő megállapításáról

(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 8. cikke (3) bekezdésére,

mivel:

(1) A 910/2014/EU rendelet 8. cikke előírja, hogy a 9. cikk (1) bekezdése szerint bejelentett elektronikus azonosítási rendszereknek meg kell határozniuk a keretükben kibocsátott elektronikus azonosító eszközök „alacsony”, „jelentős” és „magas” biztonsági szintjeit.

(2) A minimális technikai specifikációk, szabványok és eljárások meghatározása elengedhetetlen ahhoz, hogy egységesen legyenek értelmezve a biztonsági szintek részletei, valamint a bejelentett elektronikus azonosítási rendszerek nemzeti biztonsági szintjeinek a 8. cikk szerinti biztonsági szinteknek való megfeleltetésekor biztosítva legyen az átjárhatóság, ahogy azt a 910/2014/EU rendelet 12. cikke (4) bekezdésének b) pontja előírja.

(3) Az ebben a végrehajtási aktusban megállapított specifikációkhoz és eljárásokhoz – az elektronikus azonosító eszközök biztonsági szintjeinek területén rendelkezésre álló legfontosabb nemzetközi szabványként – az ISO/IEC 29115 nemzetközi szabványt vettük figyelembe. A 910/2014/EU rendelet tartalma azonban eltér ettől a nemzetközi szabványtól, különösen a személyazonosítási és személyazonosság-ellenőrzési követelmények, valamint a tagállamok személyazonosságra vonatkozó előírásai és az ugyanilyen célú meglévő uniós eszközök közötti eltérések figyelembevétele tekintetében. Tehát a melléklet, bár ezen a nemzetközi szabványon alapul, nem hivatkozhat az ISO/IEC 29115 szabvány semmilyen konkrét elemére.

(4) E rendelet a célra legmegfelelőbbnek bizonyuló, eredményalapú megközelítés alapján került kidolgozásra, ami a kifejezések és fogalmak meghatározásában is tükröződik. A fogalommeghatározások figyelembe veszik a 910/2014/EU rendeletnek az elektronikus azonosító eszközök biztonsági szintjeire vonatkozó célkitűzését. Ezért az e végrehajtási aktusban megállapított specifikációk és eljárások kialakításakor a legmesszebbmenőkig figyelembe kell venni a nagyszabású STORK kísérleti projektet, és ezen belül a projekt keretében kidolgozott előírásokat, valamint az ISO/IEC 29115 definícióit és fogalmait.

(5) Attól függően, hogy milyen kontextusban szükséges a személyazonosság bizonyítékának egy aspektusát ellenőrizni, a hiteles források többfélék lehetnek, így többek között nyilvántartások, dokumentumok, szervek. A hiteles források még hasonló kontextus esetén is eltérőek lehetnek az egyes tagállamokban.

(6) A személyazonosítási és személyazonosság-ellenőrzési követelményeknek figyelembe kell venniük a különféle rendszereket és gyakorlatokat, eközben azonban kellően biztonságosnak kell lenniük ahhoz, hogy megteremtsék a szükséges bizalmat. Az elektronikus azonosító eszközök kibocsátásától eltérő célra korábban alkalmazott eljárások elfogadását tehát függővé kell tenni annak igazolásától, hogy az eljárások megfelelnek az adott biztonsági szintre előírt követelményeknek.

[1] HL L 257., 2014.8.28., 73. o.

(7) Általában alkalmazásra kerülnek bizonyos hitelesítési tényezők, így például megosztott titkok, fizikai eszközök és fizikai attribútumok. Ösztönözni kell azonban a nagyobb számú hitelesítési tényező – különösen különféle kategóriákba tartozó tényezők – alkalmazását a hitelesítési folyamat biztonságának növelése céljából.

(8) E rendelet nem érintheti a jogi személyek képviseleti jogát. A mellékletnek azonban követelményeket kell megfogalmaznia a természetes és jogi személyek elektronikus azonosító eszközeinek összekapcsolására vonatkozólag.

(9) Fel kell ismerni az információbiztonsági és szolgáltatásirányítási rendszerek, valamint az elismert módszerek használatának és a szabványokba – így például az ISO/IEC 27000 és az ISO/IEC 20000 sorozatba – beépített elvek alkalmazásának fontosságát.

(10) A biztonsági szintekkel kapcsolatos helyes tagállami gyakorlatokat is figyelembe kell venni.

(11) A nemzetközi szabványokon alapuló informatikai biztonsági tanúsítás fontos eszköz annak ellenőrzésére, hogy a termékek biztonsági szempontból megfelelnek-e e végrehajtási aktus követelményeinek.

(12) A 910/2014/EU rendelet 48. cikkében említett bizottság az elnöke által kitűzött határidőn belül nem nyilvánított véleményt,

ELFOGADTA EZT A RENDELETET:

1. cikk

(1) A valamely bejelentett elektronikus azonosítási rendszer keretében kibocsátott elektronikus azonosító eszközökre vonatkozó „alacsony”, „jelentős” és „magas” biztonsági szinteket a mellékletben megállapított specifikációkra és eljárásokra való hivatkozással kell meghatározni.

(2) A valamely bejelentett elektronikus azonosítási rendszer keretében kibocsátott elektronikus azonosító eszközök biztonsági szintjének meghatározásához a mellékletben megállapított specifikációkat és eljárásokat kell alkalmazni, az alábbi elemek megbízhatóságának és minőségének meghatározása útján:

a) nyilvántartásba vétel, ahogy az a 910/2014/EU rendelet 8. cikke (3) bekezdésének a) pontja értelmében e rendelet mellékletének 2.1. pontjában szerepel;

b) az elektronikus azonosító eszközök irányítása, ahogy az a 910/2014/EU rendelet 8. cikke (3) bekezdésének b) és f) pontja értelmében e rendelet mellékletének 2.2. pontjában szerepel;

c) hitelesítés, ahogy az a 910/2014/EU rendelet 8. cikke (3) bekezdésének c) pontja értelmében e rendelet mellékletének 2.3. pontjában szerepel;

d) irányítás és szervezés, ahogy az a 910/2014/EU rendelet 8. cikke (3) bekezdésének d) és e) pontja értelmében e rendelet mellékletének 2.4. pontjában szerepel.

(3) Amennyiben a valamely bejelentett elektronikus azonosítási rendszer keretében kibocsátott elektronikus azonosító eszköz megfelel egy magasabb biztonsági szintnél felsorolt követelménynek, azt kell feltételezni, hogy egy alacsonyabb biztonsági szint ezzel egyenértékű követelményének is megfelel.

(4) Hacsak a melléklet vonatkozó részében másképp nem szerepel, a valamely bejelentett elektronikus azonosítási rendszer keretében kibocsátott elektronikus azonosító eszköznek az adott biztonsági szintre vonatkozóan a mellékletben felsorolt összes elemet teljesítenie kell ahhoz, hogy megfeleljen az igényelt biztonsági szintnek.

2. cikk

Ez a rendelet az *Európai Unió Hivatalos Lapjá*ban való kihirdetését követő huszadik napon lép hatályba.

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

Kelt Brüsszelben, 2015. szeptember 8-án.

a Bizottság részéről
az elnök
Jean-Claude JUNCKER

MELLÉKLET

Technikai specifikációk és eljárások a bejelentett elektronikus azonosítási rendszerek keretében kibocsátott elektronikus azonosító eszközök „alacsony”, „jelentős” és „magas” biztonsági szintjeihez

1. **Alkalmazandó fogalommeghatározások**

E melléklet alkalmazásában:

1. „hiteles forrás”: formájától függetlenül bármely megbízható forrás, amely a személyazonosság igazolásához felhasználható pontos adatokat, információkat és/vagy bizonyítékokat szolgáltat;

2. „hitelesítési tényező”: olyan tényező, amely bizonyítottan egy személyhez kapcsolódik, és amely az alábbi kategóriák valamelyikébe tartozik:

   a) „birtoklásalapú hitelesítési tényező”: olyan hitelesítési tényező, amelynél az alanynak igazolnia kell, hogy a birtokában van;

   b) „ismeretalapú hitelesítési tényező”: olyan hitelesítési tényező, amelynél az alanynak igazolnia kell, hogy ismeri;

   c) „inherens hitelesítési tényező”: olyan hitelesítési tényező, amelynek alapja egy természetes személy valamely fizikai attribútuma, és amelynél az alanynak igazolnia kell, hogy rendelkezik az adott fizikai attribútummal;

3. „dinamikus hitelesítés”: olyan elektronikus folyamat, amely kriptográfia vagy egyéb technikák alkalmazásával kérésre elektronikus igazolást készít arról, hogy az azonosító adatok az alany ellenőrzése alatt állnak vagy birtokában vannak, és amely az alany és az alany személyazonosságát igazoló rendszer közötti minden egyes hitelesítéskor változik;

4. „információbiztonsági irányítórendszer”: olyan folyamatok és eljárások összessége, amelyek kialakításának célja, hogy az információbiztonsági kockázatokat elfogadható szinten tartsa;

2. **Technikai specifikációk és eljárások**

Az e mellékletben megállapított technikai specifikációk és eljárások elemeit kell használni annak meghatározására, hogy hogyan kell alkalmazni a 910/2014/EU rendelet 8. cikkének követelményeit és kritériumait a bejelentett elektronikus azonosítási rendszer keretében kibocsátott elektronikus azonosító eszközökre.

2.1. *Nyilvántartásba vétel*

2.1.1. Igénylés és regisztráció

Biztonsági szint	Szükséges elemek
Alacsony	1. Annak biztosítása, hogy az igénylő ismeri az elektronikus azonosító eszköz használatával kapcsolatos feltételeket. 2. Annak biztosítása, hogy az igénylő ismeri az elektronikus azonosító eszköz használatával kapcsolatban ajánlott biztonsági óvintézkedéseket. 3. A személyazonosításhoz és a személyazonosság-ellenőrzéshez szükséges vonatkozó személyazonossági adatok összegyűjtése.
Jelentős	Ugyanaz, mint az alacsony szintnél.
Magas	Ugyanaz, mint az alacsony szintnél.

2.1.2. Személyazonosítás és személyazonosság-ellenőrzés (természetes személy esetén)

Biztonsági szint	Szükséges elemek
Alacsony	1. Feltételezhető, hogy a személy birtokában van egy azon tagállam által elismert bizonyítéknak, ahol az elektronikus azonosító eszköz igénylése történik, és e bizonyíték igazolja az állítólagos személyazonosságot. 2. Feltételezhető, hogy a bizonyíték valódi, vagy hogy egy hiteles forrás szerint létezik, és a bizonyíték megalapozottnak tűnik. 3. Hiteles forrás számára ismert, hogy az állítólagos személyazonosság létezik, és feltételezhető, hogy a személyazonosságot magáénak tulajdonító személy valóban az a személy.
Jelentős	Az alacsony szint, továbbá teljesíteni kell az 1–4. pontban felsorolt alternatívák egyikét: 1. Beigazolódott, hogy a személy birtokában van egy azon tagállam által elismert bizonyítéknak, ahol az elektronikus azonosító eszköz igénylése történik, és e bizonyíték igazolja az állítólagos személyazonosságot és ellenőrzésre kerül, hogy a bizonyíték valódi-e; vagy egy hiteles forrás szerint létezik-e és egy valós személyhez kapcsolható-e és lépéseket tettek annak a kockázatnak a minimalizálására, hogy a személy azonossága esetleg nem egyezik meg az állítólagos személyazonossággal, figyelembe véve például az elveszett, ellopott, felfüggesztett, visszavont vagy lejárt érvényességű bizonyítékok kockázatát; vagy 2. A regisztrációs eljárás során bemutatásra kerül egy személyazonossági okirat abban a tagállamban, ahol az okiratot kiadták, és úgy tűnik, hogy az okirat az azt bemutató személyhez tartozik és lépéseket tettek annak a kockázatnak a minimalizálására, hogy a személy azonossága esetleg nem egyezik meg az állítólagos személyazonossággal, figyelembe véve például az elveszett, ellopott, felfüggesztett, visszavont vagy lejárt érvényességű okiratok kockázatát; vagy 3. Amennyiben egy közigazgatási vagy magánszervezet által ugyanabban a tagállamban korábban elektronikus azonosító eszközök kibocsátásától eltérő célra használt eljárások egyenértékű biztonságot nyújtanak, mint a 2.1.2. pontban a jelentős biztonsági szintnél megállapítottak, akkor a regisztrációért felelős szervezetnek nem kell megismételnie azokat a korábbi eljárásokat, feltéve, hogy az egyenértékű biztonságot egy, a 765/2008/EK európai parlamenti és tanácsi rendelet [1] 2. cikkének 13. pontja szerinti megfelelőségértékelő szervezet, vagy azzal egyenértékű szervezet megerősíti; vagy 4. Amennyiben jelentős vagy magas biztonsági szintű, érvényes bejelentett elektronikus azonosító eszköz alapján és a személyazonosító adatok esetleges megváltozásában rejlő kockázatokat figyelembe véve bocsátottak ki elektronikus azonosító eszközt, akkor nem szükséges megismételni a személyazonosítási és személyazonosság-ellenőrzési folyamatokat. Amennyiben az alapként szolgáló elektronikus azonosító eszközt nem jelentették be, akkor a jelentős vagy magas biztonsági szintet egy, a 765/2008/EK rendelet 2. cikkének 13. pontja szerinti megfelelőségértékelő szervezetnek, vagy azzal egyenértékű szervezetnek meg kell erősítenie.

Biztonsági szint	Szükséges elemek
Magas	Vagy az 1., vagy a 2. pont szerinti követelményeket kell teljesíteni: 1. A jelentős szint, továbbá teljesíteni kell az a–c) pontban felsorolt alternatívák egyikét: a) Ha beigazolódott, hogy a személy birtokában van egy azon tagállam által elismert fényképes vagy biometriai azonosító bizonyítéknak, ahol az elektronikus azonosító eszköz igénylése történik, és a bizonyíték igazolja az állítólagos személyazonosságot, akkor a bizonyíték ellenőrzésre kerül, hogy megállapítsák, hogy érvényes-e egy hiteles forrás szerint; és egy hiteles forrással a személy egy vagy több fizikai tulajdonságát összehasonlítva az igénylőt azonosították az állítólagos személyazonossággal; vagy b) Amennyiben egy közigazgatási vagy magánszervezet által ugyanabban a tagállamban korábban elektronikus azonosító eszközök kibocsátásától eltérő célra használt eljárások egyenértékű biztonságot nyújtanak, mint a 2.1.2. pontban a magas biztonsági szintnél megállapítottak, akkor a regisztrációért felelős szervezetnek nem kell megismételnie azokat a korábbi eljárásokat, feltéve, hogy az egyenértékű biztonságot egy, a 765/2008/EK 2. cikkének 13. pontja szerinti megfelelőségértékelő szervezet, vagy azzal egyenértékű szervezet megerősíti; és lépéseket tesznek annak igazolására, hogy a korábbi eljárások eredményei továbbra is érvényesek; vagy c) Amennyiben magas biztonsági szintű, érvényes bejelentett elektronikus azonosító eszköz alapján és a személyazonosító adatok esetleges megváltozásában rejlő kockázatokat figyelembe véve bocsátottak ki elektronikus azonosító eszközt, akkor nem szükséges megismételni a személyazonosítási és személyazonosság-ellenőrzési folyamatokat. Amennyiben az alapként szolgáló elektronikus azonosító eszközt nem jelentették be, akkor a magas biztonsági szintet egy, a 765/2008/EK rendelet 2. cikkének 13. pontja szerinti megfelelőségértékelő szervezetnek, vagy azzal egyenértékű szervezetnek meg kell erősítenie és lépéseket tesznek annak igazolására, hogy egy bejelentett elektronikus azonosító eszköz e korábbi kibocsátási eljárásának eredményei továbbra is érvényesek. VAGY 2. Amennyiben az igénylő nem mutat be semmilyen elismert fényképes vagy biometriai azonosító bizonyítékot, akkor pontosan ugyanazokat az eljárásokat kell alkalmazni, mint amelyeket a regisztrációért felelős szervezet szerinti tagállamban nemzeti szinten alkalmaznak ilyen elismert fényképes vagy biometriai azonosító bizonyítékok megszerzéséhez.

([1]) Az Európai Parlament és a Tanács 2008. július 9-i 765/2008/EK rendelete a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről (HL L 218., 2008.8.13., 30. o.).

2.1.3. Személyazonosítás és személyazonosság-ellenőrzés (jogi személy esetén)

Biztonsági szint	Szükséges elemek
Alacsony	1. A jogi személy állítólagos személyazonossága egy azon tagállam által elismert bizonyíték alapján kerül igazolásra, ahol az elektronikus azonosító eszköz igénylése történik.

Biztonsági szint	Szükséges elemek
	2. A bizonyíték érvényesnek tűnik, és feltételezhető, hogy valódi, illetve hogy egy olyan hiteles forrás szerint létezik, amelybe a jogi személy önkéntes alapon kerül felvételre, és a felvételt a jogi személy és a hiteles forrás közötti megállapodás szabályozza. 3. A jogi személynek egy hiteles forrás szerint sem olyan a státusa, amely meggátolná abban, hogy az adott jogi személyként eljárjon.
Jelentős	Az alacsony szint, továbbá teljesíteni kell az 1–3. pontban felsorolt alternatívák egyikét: 1. A jogi személy állítólagos személyazonossága egy azon tagállam által elismert bizonyíték alapján kerül igazolásra, ahol az elektronikus azonosító eszköz igénylése történik, amely bizonyíték magában foglalja a jogi személy nevét, jogi formáját és regisztrációs számát (ha van) és a bizonyíték ellenőrzésre kerül annak megállapítására, hogy valódi-e, vagy hogy létezik-e egy olyan hiteles forrás szerint, amelybe a jogi személynek kötelezően be kell kerülnie ahhoz, hogy ágazatában működhessen és lépéseket tettek azon kockázat minimalizálására, hogy a jogi személy azonossága esetleg nem egyezik meg az állítólagos személyazonossággal, figyelembe véve például az elveszett, ellopott, felfüggesztett, visszavont vagy lejárt érvényességű okiratok kockázatát; vagy 2. Amennyiben egy közigazgatási vagy magánszervezet által ugyanabban a tagállamban korábban elektronikus azonosító eszközök kibocsátásától eltérő célra használt eljárások egyenértékű biztonságot nyújtanak, mint a 2.1.3. pontban a jelentős biztonsági szintnél megállapítottak, akkor a regisztrációért felelős szervezetnek nem kell megismételnie azokat a korábbi eljárásokat, feltéve, hogy az egyenértékű biztonságot egy, a 765/2008/EK rendelet 2. cikkének 13. pontja szerinti megfelelőségértékelő szervezet, vagy azzal egyenértékű szervezet megerősíti; vagy 3. Amennyiben jelentős vagy magas biztonsági szintű, érvényes bejelentett elektronikus azonosító eszköz alapján bocsátottak ki elektronikus azonosító eszközt, nem szükséges megismételni a személyazonosítási és személyazonosság-ellenőrzési folyamatokat. Amennyiben az alapként szolgáló elektronikus azonosító eszközt nem jelentették be, akkor a jelentős vagy magas biztonsági szintet egy, a 765/2008/EK rendelet 2. cikkének 13. pontja szerinti megfelelőségértékelő szervezetnek, vagy azzal egyenértékű szervezetnek kell megerősítenie.
Magas	A jelentős szint, továbbá teljesíteni kell az 1–3. pontban felsorolt alternatívák egyikét: 1. A jogi személy állítólagos személyazonossága egy azon tagállam által elismert bizonyíték alapján kerül igazolásra, ahol az elektronikus azonosító eszköz igénylése történik, amely bizonyíték magában foglalja a jogi személy nevét, jogi formáját és legalább egy egyedi azonosítót, ami a jogi személyt nemzeti kontextusban azonosítja és ellenőrzésre kerül, hogy a bizonyíték egy hiteles forrás szerint érvényes-e; vagy

Biztonsági szint	Szükséges elemek
	2. Amennyiben egy közigazgatási vagy magánszervezet által ugyanabban a tagállamban korábban elektronikus azonosító eszközök kibocsátásától eltérő célra használt eljárások egyenértékű biztonságot nyújtanak, mint a 2.1.3. pontban a magas biztonsági szintnél megállapítottak, akkor a regisztrációért felelős szervezetnek nem kell megismételnie azokat a korábbi eljárásokat, feltéve, hogy az egyenértékű biztonságot egy, a 765/2008/EK rendelet 2. cikkének 13. pontja szerinti megfelelőségértékelő szervezet, vagy azzal egyenértékű szervezet megerősíti és lépéseket tesznek annak igazolására, hogy az említett korábbi eljárás eredményei továbbra is érvényesek; vagy 3. Amennyiben magas biztonsági szintű, érvényes bejelentett elektronikus azonosító eszköz alapján bocsátottak ki elektronikus azonosító eszközt, nem szükséges megismételni a személyazonosítási és személyazonosság-ellenőrzési folyamatokat. Amennyiben az alapként szolgáló elektronikus azonosító eszközt nem jelentették be, akkor a magas biztonsági szintet egy, a 765/2008/EK európai parlamenti és tanácsi rendelet 2. cikkének 13. pontja szerinti megfelelőségértékelő szervezetnek, vagy azzal egyenértékű szervezetnek kell megerősítenie és lépéseket tesznek annak igazolására, hogy egy bejelentett elektronikus azonosító eszköz e korábbi kibocsátási eljárásának eredményei továbbra is érvényesek.

2.1.4. Természetes és jogi személyek elektronikus azonosító eszközeinek egymáshoz rendelése

Egy természetes személy elektronikus azonosító eszközének és egy jogi személy elektronikus azonosító eszközének egymáshoz rendelésére megfelelő esetben az alábbi feltételek vonatkoznak:

1. Meg kell lennie a lehetőségnek az egymáshoz rendelés felfüggesztésére és/vagy visszavonására. Az egymáshoz rendelés életciklusának (pl. aktiválás, felfüggesztés, megújítás, visszavonás) kezelése nemzeti szinten elismert eljárások szerint történik.

2. Az a természetes személy, akinek elektronikus azonosító eszköze hozzá van rendelve a jogi személy elektronikus azonosító eszközéhez, nemzeti szinten elismert eljárások alapján más természetes személyre ruházhatja át az egymáshoz rendelés gyakorlását. Az átruházó természetes személy azonban felelősségre vonható marad.

3. Az egymáshoz rendelés az alábbi módon történik:

Biztonsági szint	Szükséges elemek
Alacsony	1. Ellenőrzésre került, hogy a jogi személy nevében eljáró természetes személy személyazonosságának igazolása alacsony vagy afeletti szinten történt. 2. Az egymáshoz rendelés nemzeti szinten elismert eljárások alapján történt. 3. A természetes személynek egy hiteles forrás szerint sem olyan a státusa, amely meggátolná a személyt abban, hogy a jogi személy nevében eljárjon.
Jelentős	Az alacsony szint 3. pontja, továbbá: 1. Ellenőrzésre került, hogy a jogi személy nevében eljáró természetes személy személyazonosságának igazolása jelentős vagy magas szinten történt.

Biztonsági szint	Szükséges elemek
	2. Az egymáshoz rendelés nemzeti szinten elismert eljárások alapján történt, és ennek eredményeként egy hiteles forrás regisztrálta az egymáshoz rendelést. 3. Az egymáshoz rendelés hiteles forrásból származó információk alapján került ellenőrzésre.
Magas	Az alacsony szint 3. pontja és a jelentős szint 2. pontja, továbbá: 1. Ellenőrzésre került, hogy a jogi személy nevében eljáró természetes személy személyazonosságának igazolása magas szinten történt. 2. Az egymáshoz rendelés ellenőrzése egy, a jogi személyhez nemzeti kontextusban tartozó egyedi azonosító alapján, és hiteles forrásból származó, a természetes személyt egyedileg azonosító információk alapján történt.

2.2. *Az elektronikus azonosító eszközök irányítása*

2.2.1. Az elektronikus azonosító eszközök jellemzői és kialakítása

Biztonsági szint	Szükséges elemek
Alacsony	1. Az elektronikus azonosító eszköz legalább egy hitelesítési tényezőt alkalmaz. 2. Az elektronikus azonosító eszköz úgy van kialakítva, hogy a kibocsátó ésszerű lépéseket tesz annak ellenőrzésére, hogy az eszközt kizárólag annak a személynek az ellenőrzése alatt vagy birtokában használják-e, akihez az eszköz tartozik.
Jelentős	1. Az elektronikus azonosító eszköz legalább két, különböző kategóriába tartozó hitelesítési tényezőt alkalmaz. 2. Az elektronikus azonosító eszköz úgy van kialakítva, hogy feltételezhető, hogy csak annak a személynek az ellenőrzése alatt vagy birtokában használják, akihez az eszköz tartozik.
Magas	A jelentős szint, továbbá: 1. Az elektronikus azonosító eszköz védelmet nyújt a másolással és manipulációval, valamint a nagy támadási potenciálú támadókkal szemben. 2. Az elektronikus azonosító eszköz úgy van kialakítva, hogy az a személy, akihez az eszköz tartozik, bizonyosan meg tudja védeni az eszközt attól, hogy mások használják.

2.2.2. Kibocsátás, átadás és aktiválás

Biztonsági szint	Szükséges elemek
Alacsony	A kibocsátást követően az elektronikus azonosító eszköz átadása egy olyan mechanizmus révén történik, amellyel feltételezhetően csak a célszemélyt érik el.
Jelentős	A kibocsátást követően az elektronikus azonosító eszköz átadása egy olyan mechanizmus révén történik, amellyel az átadás feltételezhetően csak annak a személynek a birtokába történik, akihez az eszköz tartozik.
Magas	Az aktiválási folyamat ellenőrzi, hogy az elektronikus azonosító eszköz átadása csak annak a személynek a birtokába történt, akihez az tartozik.

2.2.3. Felfüggesztés, visszavonás és újraaktiválás

Biztonsági szint	Szükséges elemek
Alacsony	1. Az elektronikus azonosító eszközt rövid időn belül és hatékony módon fel lehet függeszteni és/vagy vissza lehet vonni. 2. Meghozták az illetéktelen felfüggesztés, visszavonás és/vagy újraaktiválás megakadályozásához szükséges intézkedéseket. 3. Újraaktiválásra csak akkor kerülhet sor, ha a felfüggesztés vagy visszavonás előtt érvényes biztonsági követelmények továbbra is teljesülnek.
Jelentős	Ugyanaz, mint az alacsony szintnél.
Magas	Ugyanaz, mint az alacsony szintnél.

2.2.4. Megújítás és csere

Biztonsági szint	Szükséges elemek
Alacsony	A személyazonosító adatok esetleges megváltozásában rejlő kockázatokat figyelembe véve a megújításnak vagy cserének ugyanazoknak a biztonsági követelményeknek kell megfelelnie, mint a kiindulási személyazonosításnak és személyazonosság-ellenőrzésnek, vagy egy azonos vagy magasabb biztonsági szintű, érvényes elektronikus azonosító eszközön kell alapulnia.
Jelentős	Ugyanaz, mint az alacsony szintnél.
Magas	Az alacsony szint, továbbá: Ha a megújítás vagy csere érvényes elektronikus azonosító eszköz alapján történik, a személyazonossági adatokat egy hiteles forrásban ellenőrizni kell.

2.3. *Hitelesítés*

E pontban a hitelesítési mechanizmus alkalmazásához kapcsolódó veszélyekre összpontosítunk, és felsoroljuk az egyes biztonsági szintek követelményeit. E pont alkalmazásában úgy kell értelmezni, hogy az ellenőrzéseknek arányban kell állniuk az adott szinthez tartozó kockázatokkal.

2.3.1. Hitelesítési mechanizmus

Az alábbi táblázatban biztonsági szintenként adjuk meg az azon hitelesítési mechanizmusra vonatkozó követelményeket, amelynek keretében a természetes vagy jogi személy az elektronikus azonosító eszközzel személyazonosságát igazolja az igénybe vevő fél számára.

Biztonsági szint	Szükséges elemek
Alacsony	1. A személyazonossági adatok kiadása előtt megbízható módon ellenőrzésre kerül az elektronikus azonosító eszköz és annak érvényessége. 2. Amennyiben a személyazonossági adatokat a hitelesítési mechanizmus részeként tárolják, ott biztosítva van, hogy ez az információ ne vesszen el és ne legyen veszélyeztetve, ideértve az offline analízist. 3. A hitelesítési mechanizmus biztonsági ellenőrzéseket végez az elektronikus azonosító eszközök ellenőrzéséhez azért, hogy ily módon minimálisra csökkentse annak valószínűségét, hogy olyan módszerekkel, mint a találgatás, a lehallgatás, vagy a kommunikáció visszajátszása, illetve manipulálása egy közepes-alapszintű támadási potenciállal rendelkező támadó meghiúsítja a hitelesítési mechanizmust.

Biztonsági szint	Szükséges elemek
Jelentős	Az alacsony szint, továbbá: 1. A személyazonossági adatok kiadása előtt megbízható módon, dinamikus hitelesítés révén ellenőrzésre kerül az elektronikus azonosító eszköz és annak érvényessége. 2. A hitelesítési mechanizmus biztonsági ellenőrzéseket végez az elektronikus azonosító eszközök ellenőrzéséhez azért, hogy ily módon minimálisra csökkentse annak valószínűségét, hogy olyan módszerekkel, mint a találgatás, a lehallgatás, vagy a kommunikáció visszajátszása, illetve manipulálása egy mérsékelt támadási potenciálú támadó meghiúsítja a hitelesítési mechanizmust.
Magas	A jelentős szint, valamint: A hitelesítési mechanizmus biztonsági ellenőrzéseket végez az elektronikus azonosító eszközök ellenőrzéséhez azért, hogy ily módon minimálisra csökkentse annak valószínűségét, hogy olyan módszerekkel, mint a találgatás, a lehallgatás, vagy a kommunikáció visszajátszása, illetve manipulálása egy magas támadási potenciálú támadó meghiúsítja a hitelesítési mechanizmust.

2.4. *Irányítás és szervezés*

A határokon átnyúló elektronikus azonosításhoz kapcsolódó szolgáltatásokat nyújtó összes résztvevőnek („szolgáltató") dokumentált információbiztonság-irányítási gyakorlatokat, politikákat, kockázatkezelési módszereket és egyéb elismert ellenőrzéseket kell alkalmaznia, hogy biztosítékkal szolgáljanak az adott tagállamban az elektronikus azonosítási rendszerekért felelős megfelelő irányító szervek számára arról, hogy hatékony gyakorlatokat alkalmaznak. A 2.4. pontban úgy kell értelmezni, hogy az összes követelménynek/elemnek arányban kell állnia az adott szinthez tartozó kockázatokkal.

2.4.1. Általános rendelkezések

Biztonsági szint	Szükséges elemek
Alacsony	1. Az e rendelet hatálya alá tartozó bármilyen operatív szolgáltatást nyújtó szolgáltatók közigazgatási hatóságok vagy valamely tagállam nemzeti törvényei által ilyenként elismert jogi személyek, amelyek kialakított szervezettel rendelkeznek, és a szolgáltatások nyújtása szempontjából releváns valamennyi részük teljes mértékben működőképes. 2. A szolgáltatók a szolgáltatás működtetésével és nyújtásával kapcsolatban rájuk vonatkozó összes törvényi követelménynek megfelelnek, ideértve a kért információk típusára, a személyazonosság igazolásának módjára, valamint arra vonatkozó követelményeket, hogy milyen információk őrizhetők meg és mennyi ideig. 3. A szolgáltatók bizonyítani tudják, hogy képesek vállalni a károkozási felelősség kockázatát, továbbá elegendő anyagi eszközzel rendelkeznek a folyamatos működéshez és a szolgáltatások nyújtásához. 4. A szolgáltatók felelősséggel tartoznak a más szervezethez kiszervezett valamennyi kötelezettség teljesítéséért, valamint a rendszer előírásainak oly módon történő betartásáért, mintha maguk végezték volna el a feladatokat. 5. A nem a nemzeti törvények alapján létrehozott elektronikus azonosítási rendszerek esetében hatékony lezárási terv szükséges. Ennek a tervnek tartalmaznia kell a szolgáltatás rendezett befejezését vagy más szolgáltató általi folytatását, az illetékes hatóságok és a végfelhasználók tájékoztatásának módját, valamint azt, hogy a rendszer előírásaival összhangban hogyan kell az eltárolt adatokat megvédeni, megőrizni vagy megsemmisíteni.
Jelentős	Ugyanaz, mint az alacsony szintnél.
Magas	Ugyanaz, mint az alacsony szintnél.

2.4.2. Értesítések közzététele és felhasználói tájékoztatás

Biztonsági szint	Szükséges elemek
Alacsony	1. A szolgáltatás meghatározásának közzététele, amelyben szerepel az összes alkalmazandó feltétel és díj, a használatra vonatkozó összes korlátozást is ideértve. A szolgáltatás meghatározásának tartalmaznia kell az adatvédelmi szabályokat is. 2. Megfelelő szabályokat és eljárásokat kell bevezetni annak érdekében, hogy a szolgáltatás felhasználói kellő időben és megbízható módon értesüljenek magának a szolgáltatásnak a meghatározását vagy az alkalmazandó feltételeket és az adott szolgáltatásra vonatkozó adatvédelmi szabályokat érintő bármely változásról. 3. Megfelelő szabályokat és eljárásokat kell bevezetni, amelyek alapján teljes körű és pontos válaszok adhatók a tájékoztatáskérésekre.
Jelentős	Ugyanaz, mint az alacsony szintnél.
Magas	Ugyanaz, mint az alacsony szintnél.

2.4.3. Információbiztonsági irányítás

Biztonsági szint	Szükséges elemek
Alacsony	Az információbiztonsági kockázatok kezelésére és ellenőrzésére hatékony információbiztonsági irányítórendszer áll rendelkezésre.
Jelentős	Az alacsony szint, továbbá: Az információbiztonsági irányítórendszer az információbiztonsági kockázatok kezelése és ellenőrzése során bevált normákhoz vagy elvekhez igazodik.
Magas	Ugyanaz, mint a jelentős szintnél.

2.4.4. Nyilvántartás

Biztonsági szint	Szükséges elemek
Alacsony	1. A vonatkozó információk rögzítése és tárolása hatékony nyilvántartás-kezelő rendszer alkalmazásával, az adatvédelemmel és az adatmegőrzéssel kapcsolatos alkalmazandó jogszabályokat és helyes gyakorlatot is figyelembe véve. 2. Az eltárolt adatok megőrzése, ameddig a nemzeti törvények vagy más nemzeti adminisztratív rendelkezések megengedik, és védelme, ameddig azok a biztonság megsértéseinek auditálása vagy vizsgálata, továbbá megőrzés céljára szükségesek, amelyet követően az eltárolt adatokat biztonságosan meg kell semmisíteni.
Jelentős	Ugyanaz, mint az alacsony szintnél.
Magas	Ugyanaz, mint az alacsony szintnél.

2.4.5. Létesítmények és személyzet

Az alábbi táblázat az esetleges olyan alvállalkozók létesítményeire és személyzetére vonatkozó követelményeket ismerteti, akik e rendelet hatálya alá tartozó feladatokat végeznek. Az egyes követelmények betartásának arányosnak kell lennie a nyújtott biztonsági szinthez kapcsolódó kockázatok szintjével.

Biztonsági szint	Szükséges elemek
Alacsony	1. Olyan eljárások megléte, amelyek biztosítják, hogy a személyzet és az alvállalkozók az általuk elvégzendő feladatokhoz szükséges képességek tekintetében kellő képzettséggel, szakképzettséggel és tapasztalattal rendelkeznek. 2. Elegendő személyzet és alvállalkozó megléte a szolgáltatásnak a saját előírásai és eljárásai szerinti működtetéséhez és erőforrásokkal való ellátásához. 3. A szolgáltatás nyújtásához használt létesítményeket folyamatosan felügyelik és védik a környezeti események, illetéktelen hozzáférés és más tényezők okozta károk ellen, amelyek befolyással lehetnek a szolgáltatás biztonságára. 4. A szolgáltatás nyújtásához használt létesítmények biztosítják, hogy kizárólag a személyzet vagy az alvállalkozók juthassanak be a személyes, kriptográfiás vagy egyéb bizalmas információkat tároló vagy feldolgozó területekre.
Jelentős	Ugyanaz, mint az alacsony szintnél.
Magas	Ugyanaz, mint az alacsony szintnél.

2.4.6. Technikai ellenőrzések

Biztonsági szint	Szükséges elemek
Alacsony	1. Arányos technikai ellenőrzések megléte a szolgáltatások biztonságát, valamint a feldolgozott információk bizalmas jellegét, sértetlenségét és rendelkezésre állását veszélyeztető kockázatok kezelésére. 2. A személyes vagy érzékeny információk cseréjéhez használt elektronikus kommunikációs csatornák védve vannak a lehallgatás, manipuláció és visszajátszás ellen. 3. Az érzékeny kriptográfiai anyagokhoz való hozzáférés, amennyiben elektronikus azonosító eszközök kibocsátásához és hitelesítéshez használják, kizárólag a szigorúan hozzáférést igénylő szerepekre és alkalmazásokra korlátozódik. Biztosítani kell, hogy az ilyen anyagokat ne tárolják hosszabb ideig egyszerű szöveg formájában. 4. Vannak olyan eljárások, amelyek biztosítják, hogy az idő előrehaladtával ne csökkenjen a biztonság mértéke, és hogy megfelelő megoldások álljanak rendelkezésre a kockázati szintek változásaira, a biztonsági eseményekre és a biztonság megsértéseire vonatkozóan. 5. A személyes, kriptográfiás vagy egyéb bizalmas információkat tartalmazó összes adathordozót biztonságos módon tárolják, szállítják és ártalmatlanítják.
Jelentős	Ugyanaz, mint az alacsony szintnél, valamint: Bizalmas kriptográfiai anyagok, amennyiben azokat elektronikus azonosító eszközök kibocsátásához és hitelesítéshez használják, a manipuláció ellen védettek.
Magas	Ugyanaz, mint a jelentős szintnél.

2.4.7. Megfelelőség és audit

Biztonsági szint	Szükséges elemek
Alacsony	Olyan rendszeres belső auditok elvégzése, amelyek a szolgáltatás nyújtásával kapcsolatos összes részre kiterjednek és biztosítják a vonatkozó előírások betartását.

Biztonsági szint	Szükséges elemek
Jelentős	Olyan rendszeres független belső vagy külső auditok elvégzése, amelyek a szolgáltatás nyújtásával kapcsolatos összes részre kiterjednek és biztosítják a vonatkozó előírások betartását.
Magas	1. Olyan rendszeres független külső auditok elvégzése, amelyek a szolgáltatás nyújtásával kapcsolatos összes részre kiterjednek és biztosítják a vonatkozó előírások betartását. 2. Amennyiben egy rendszert közvetlenül egy kormányzati szerv irányít, akkor a rendszer auditálása a nemzeti jogszabályokkal összhangban történik.

A BIZOTTSÁG (EU) 2015/1503 VÉGREHAJTÁSI RENDELETE

(2015. szeptember 8.)

az egyes gyümölcs- és zöldségfélék behozatali árának meghatározására szolgáló behozatali átalányértékek megállapításáról

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a mezőgazdasági termékpiacok közös szervezésének létrehozásáról, és a 922/72/EGK, a 234/79/EK, az 1037/2001/EK és az 1234/2007/EK tanácsi rendelet hatályon kívül helyezéséről szóló, 2013. december 17-i 1308/2013/EU európai parlamenti és tanácsi rendeletre ([1]),

tekintettel az 1234/2007/EK tanácsi rendeletnek a gyümölcs- és zöldség-, valamint a feldolgozottgyümölcs- és feldolgozottzöldség-ágazatra alkalmazandó részletes szabályainak a megállapításáról szóló, 2011. június 7-i 543/2011/EU bizottsági végrehajtási rendeletre ([2]) és különösen annak 136. cikke (1) bekezdésére,

mivel:

(1) Az Uruguayi Forduló többoldalú kereskedelmi tárgyalásai eredményeinek megfelelően az 543/2011/EU végrehajtási rendelet a XVI. mellékletének A. részében szereplő termékek és időszakok tekintetében meghatározza azokat a szempontokat, amelyek alapján a Bizottság rögzíti a harmadik országokból történő behozatalra vonatkozó átalányértékeket.

(2) Az 543/2011/EU végrehajtási rendelet 136. cikke (1) bekezdése alapján a behozatali átalányérték számítására munkanaponként, változó napi adatok figyelembevételével kerül sor. Ezért helyénvaló előírni, hogy e rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetésének napján lépjen hatályba,

ELFOGADTA EZT A RENDELETET:

1. cikk

Az 543/2011/EU végrehajtási rendelet 136. cikkében említett behozatali átalányértékeket e rendelet melléklete határozza meg.

2. cikk

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetésének napján lép hatályba.

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

Kelt Brüsszelben, 2015. szeptember 8-án.

a Bizottság részéről,
az elnök nevében,
Jerzy PLEWA
mezőgazdasági és vidékfejlesztési főigazgató

([1]) HL L 347., 2013.12.20., 671. o.
([2]) HL L 157., 2011.6.15., 1. o.

MELLÉKLET

Az egyes gyümölcs- és zöldségfélék behozatali árának meghatározására szolgáló behozatali átalányértékek

(EUR/100 kg)

KN-kód	Országkód (1)	Behozatali átalányérték
0702 00 00	MA	173,3
	MK	48,7
	XS	41,5
	ZZ	87,8
0707 00 05	MK	76,3
	TR	116,3
	XS	42,0
	ZZ	78,2
0709 93 10	TR	133,1
	ZZ	133,1
0805 50 10	AR	135,9
	BO	135,7
	CL	125,5
	UY	142,2
	ZA	136,9
	ZZ	135,2
0806 10 10	EG	239,8
	MK	63,9
	TR	129,5
	ZZ	144,4
0808 10 80	AR	188,7
	BR	93,9
	CL	134,4
	NZ	143,4
	US	112,5
	UY	110,5
	ZA	117,6
	ZZ	128,7
0808 30 90	AR	131,9
	CL	100,0
	TR	122,9
	ZA	113,5
	ZZ	117,1
0809 30 10, 0809 30 90	MK	80,1
	TR	141,7
	ZZ	110,9

(EUR/100 kg)

KN-kód	Országkód (1)	Behozatali átalányérték
0809 40 05	BA	54,8
	IL	336,8
	MK	44,1
	XS	70,3
	ZZ	126,5

(1) Az országoknak a Közösség harmadik országokkal folytatott külkereskedelmére vonatkozó statisztikáról szóló 471/2009/EK európai parlamenti és tanácsi rendeletnek az országok és területek nómenklatúrájának frissítése tekintetében történő végrehajtásáról szóló, 2012. november 27-i 1106/2012/EU bizottsági rendeletben (HL L 328., 2012.11.28., 7. o.) meghatározott nómenklatúrája szerint. A „ZZ” jelentése „egyéb származás”.

HATÁROZATOK

A BIZOTTSÁG (EU) 2015/1504 VÉGREHAJTÁSI HATÁROZATA

(2015. szeptember 7.)

az energiastatisztikáról szóló 1099/2008/EK európai parlamenti és tanácsi rendelet szerinti statisztikai adatszolgáltatásra vonatkozóan egyes tagállamok részére engedélyezett eltérések biztosításáról

(az értesítés a C(2015) 6105. számú dokumentummal történt)

(Csak az észt, francia, görög, holland és szlovák nyelvű szöveg hiteles)

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel az energiastatisztikáról szóló, 2008. október 22-i 1099/2008/EK európai parlamenti és tanácsi rendeletre ([1]) és különösen annak 5. cikke (4) bekezdésére és 10. cikke (2) bekezdésére,

mivel:

(1) Az 1099/2008/EK rendelet 5. cikkének (4) bekezdése értelmében valamely tagállam megfelelően indokolt kérésére eltérések biztosíthatók a nemzeti statisztikák azon részei alól, amelyek összegyűjtése a válaszadókra túlzott terheket róna.

(2) Belgium, Észtország, Ciprus és Szlovákia eltérés engedélyezését kérte bizonyos referenciaévek tekintetében a háztartások energiafogyasztására vonatkozó, a végső felhasználás típusa szerinti részletes statisztika elkészítése alól.

(3) Az érintett tagállamok által rendelkezésre bocsátott információk indokolják az eltérések engedélyezését.

(4) Az e határozatban előírt intézkedések összhangban vannak az európai statisztikai rendszer bizottságának véleményével,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

Az 1099/2008/EK rendelet rendelkezéseitől a következő eltéréseket kell engedélyezni:

1. Belgium számára eltérés engedélyezett a 2015-ös referenciaév eredményeinek benyújtása tekintetében a háztartások részletes energiafelhasználására vonatkozóan a végfelhasználás típusa szerint (az A. melléklet 26. pontjának 2.3. alpontja szerinti meghatározással: „Egyéb ágazatok – Lakossági fogyasztás”), a B. melléklet 1.2.3. pontjának 4.2.1–4.2.5. pontja, 2.2.3. pontjának 4.2.1–4.2.5. pontja, 3.2.3. pontjának 3.1–3.6. pontja, 4.2.3. pontjának 7.2.1–7.2.5. pontja, és 5.2.4. pontjának 4.2.1 – 4.2.5. pontja esetében.

([1]) HL L 304., 2008.11.14., 1. o.

2. Észtország számára eltérés engedélyezett a 2015-ös, 2016-os és 2017-es referenciaév eredményeinek benyújtása tekintetében a háztartások részletes energiafelhasználására vonatkozóan a végfelhasználás típusa szerint (az A. melléklet 26. pontjának 2.3. alpontja szerinti meghatározással: „Egyéb ágazatok – Lakossági fogyasztás"), a B. melléklet 1.2.3. pontjának 4.2.1–4.2.5. pontja, 2.2.3. pontjának 4.2.1–4.2.5. pontja, 3.2.3. pontjának 3.1–3.6. pontja, 4.2.3. pontjának 7.2.1–7.2.5. pontja, és 5.2.4. pontjának 4.2.1–4.2.5. pontja esetében.

3. Ciprus számára eltérés engedélyezett a 2015-ös, 2016-os és 2017-es referenciaév eredményeinek benyújtása tekintetében a háztartások részletes energiafelhasználására vonatkozóan a végfelhasználás típusa szerint (az A. melléklet 26. pontjának 2.3. pontja szerinti meghatározással: „Egyéb ágazatok – Lakossági fogyasztás"), a B. melléklet 1.2.3. pontjának 4.2.1.–4.2.5. pontja, 2.2.3. pontjának 4.2.1.–4.2.5. pontja, 3.2.3. pontjának 3.1–3.6. pontja, és 5.2.4. pontjának 4.2.1.–4.2.5. pontja esetében.

4. Szlovákia számára eltérés engedélyezett a 2015-ös és 2016-es referenciaév eredményeinek benyújtása tekintetében a háztartások részletes energiafelhasználására vonatkozóan a végfelhasználás típusa szerint (az A. melléklet 26. pontjának 2.3. pontja szerinti meghatározással: „Egyéb ágazatok – Lakossági fogyasztás"), a B. melléklet 1.2.3. pontjának 4.2.1.–4.2.5. pontja, 2.2.3. pontjának 4.2.1–4.2.5. pontja, 3.2.3. pontjának 3.1–3.6. pontja, 4.2.3. pontjának 7.2.1.–7.2.5. pontja, és 5.2.4. pontjának 4.2.1.–4.2.5. pontja esetében.

2. cikk

Ennek a határozatnak Belga Királyság, az Észt Köztársaság, a Ciprusi Köztársaság és a Szlovák Köztársaság a címzettje.

Kelt Brüsszelben, 2015. szeptember 7-én.

a Bizottság részéről
Marianne THYSSEN
a Bizottság tagja

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 határokon 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) preambulumbekezdésével 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 specifikációnak.

---

[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 Lapjá*ban 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 hatályon 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:

a) 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. akkreditálási) 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 hatályon kívül helyezéséről szóló, 2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendeletben meghatározott vonatkozó rendelkezések szerint.

Az elektronikus aláírások határokon 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 tartalmazzák.

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 910/210/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 értékelik 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 információnak – 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”.

A BIZOTTSÁG (EU) 2015/1506 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 27. cikkének (5) bekezdése és 37. cikkének (5) bekezdése szerint a közigazgatási szervek által elismert fokozott biztonságú elektronikus aláírások és fokozott biztonságú bélyegzők formátumaira vonatkozó specifikációk 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 27. cikke (5) bekezdésére és 37. cikkének (5) bekezdésére,

mivel:

(1) A tagállamoknak ki kell alakítaniuk az olyan szükséges technikai eszközöket, amelyek lehetővé teszik számukra a közigazgatási szervek által vagy azok nevében felajánlott online szolgáltatások használatakor szükséges elektronikusan aláírt dokumentumok feldolgozását.

(2) A 910/2014/EU rendelet előírja, hogy a közigazgatási szervek által vagy azok nevében nyújtott online szolgáltatások használatához fokozott biztonságú elektronikus aláírás vagy bélyegző használatát előíró tagállamoknak el kell ismerniük a fokozott biztonságú elektronikus aláírásokat és bélyegzőket, a minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírásokat és bélyegzőket, és a meghatározott formátumú, vagy meghatározott referencia-módszerekkel hitelesített alternatív formátumú minősített elektronikus aláírásokat és bélyegzőket.

(3) Az adott formátumok és referencia-módszerek meghatározásakor figyelembe kell venni a meglévő gyakorlatokat, szabványokat és uniós jogi aktusokat.

(4) A 2014/148/EU bizottsági végrehajtási határozat ([2]) meghatározott egy sor fokozott biztonságú elektronikus aláírás-formátumot a legelterjedtebbek közül, amelyeket a tagállamoknak technikailag támogatniuk kell, ha az online közigazgatási eljárásokhoz fokozott biztonságú elektronikus aláírás szükséges. A referenciaformátumok létrehozása azt a célt szolgálja, hogy megkönnyítse az elektronikus aláírások határokon átnyúló hitelesítését és javítsa az elektronikus eljárások határokon átnyúló átjárhatóságát.

(5) Az e határozat mellékletében felsorolt szabványok a fokozott biztonságú elektronikus aláírások formátumaira vonatkozó meglévő szabványok. A hivatkozott formátumok hosszú távú archiválási formáit a szabványügyi szervek jelenleg vizsgálják felül, ezért a hosszú távú archiválás részleteit meghatározó szabványok nem tartoznak e határozat hatálya alá. Ha majd rendelkezésre áll a hivatkozott szabványok új verziója, akkor a hosszú távú archiválással kapcsolatos szabványokra és rendelkezésekre történő hivatkozások is felülvizsgálatra kerülnek.

(6) A fokozott biztonságú elektronikus aláírások és a fokozott biztonságú elektronikus bélyegzők technikai szempontból hasonlóak egymáshoz. Ezért a fokozott biztonságú elektronikus aláírások formátumaira vonatkozó szabványokat értelemszerűen kell alkalmazni a fokozott biztonságú elektronikus bélyegzőkre is.

(7) Amennyiben a technikailag általánosan támogatott formátumoktól eltérő elektronikus aláírás- vagy bélyegzőformátumokat alkalmaznak az aláírásra, illetve bélyegzésre, akkor az elektronikus aláírások, illetve bélyegzők határokon átnyúló ellenőrzését lehetővé tevő hitelesítési eszközt kell biztosítani. Ahhoz, hogy a fogadó tagállam megbízhasson más tagállamok hitelesítési eszközeiben, könnyen elérhető tájékoztatást kell biztosítani ezekről a hitelesítési eszközökről az elektronikus dokumentumokban, az elektronikus aláírásokban vagy az elektronikus dokumentumkonténerekben.

([1]) HL L 257., 2014.8.28., 73. o.

([2]) A Bizottság 2014. március 17-i 2014/148/EU végrehajtási határozata az illetékes hatóságok által a belső piaci szolgáltatásokról szóló 2006/123/EK európai parlamenti és tanácsi irányelv alapján elektronikusan aláírt dokumentumok országhatáron átnyúló feldolgozására vonatkozó minimumkövetelményekről szóló 2011/130/EU határozat módosításáról. (HL L 80., 2014.3.19., 7. o.)

(8) Amennyiben egy tagállam közigazgatási szolgáltatásaiban rendelkezésre állnak automatizált feldolgozásra alkalmas elektronikusaláírás- vagy -bélyegzőhitelesítési lehetőségek, a fogadó tagállam számára is elérhetővé kell tenni és biztosítani kell az ilyen hitelesítési lehetőségeket. Mindazonáltal e határozat nem gátolhatja meg a 910/2014/EU rendelet 27. cikke (1) és (2) bekezdésének, valamint 37. cikke (1) és (2) bekezdéseinek alkalmazását akkor, ha alternatív módszerek esetén a hitelesítési lehetőségek automatizált feldolgozása nem lehetséges.

(9) Ahhoz, hogy összehasonlítható követelményeket biztosítsunk a hitelesítéshez és fokozzuk a bizalmat az általánosan támogatottaktól eltérő elektronikus aláírás- és bélyegzőformátumokhoz a tagállamok által biztosított hitelesítési lehetőségekben, a hitelesítési eszközökre e határozatban megállapított követelmények a 910/2014/EU rendelet 32. és 40. cikkében említett, a minősített elektronikus aláírások és bélyegzők hitelesítésére vonatkozó követelményeket veszik alapul.

(10) Az e határozatban előírt intézkedések összhangban vannak a 910/2014/EU rendelet 48. cikkével létrehozott bizottság véleményével,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

A 910/2014/EU rendelet 27. cikkének (1) és (2) bekezdése szerint fokozott biztonságú elektronikus aláírást vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírást előíró tagállamok elismerik az XML, CMS és PDF formátumú, B, T vagy LT megfelelőségi szintű fokozott biztonságú elektronikus aláírásokat, valamint a kapcsolódó aláírás-konténert tartalmazó fokozott biztonságú elektronikus aláírásokat, amennyiben az aláírások megfelelnek a mellékletben foglalt technikai specifikációnak.

2. cikk

(1) A 910/2014/EU rendelet 27. cikkének (1) és (2) bekezdése szerint fokozott biztonságú elektronikus aláírást vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírást előíró tagállamok elismernek az e határozat 1. cikkében említett elektronikus aláírás-formátumoktól eltérő formátumokat is, feltéve, hogy az aláíró által igénybe vett bizalmi szolgáltató székhelye szerinti tagállam más tagállamoknak aláírás-hitelesítési lehetőségeket kínál, amelyek lehetőség szerint alkalmasak automatizált feldolgozásra.

(2) Az aláírás-hitelesítési lehetőségeknek:

a) lehetővé kell tenniük a tagállamok számára, hogy online, ingyenesen és a nyelvet nem beszélők számára is érthetően hitelesítsék a kapott elektronikus aláírásokat;

b) meg kell jelenniük az aláírt dokumentumban, az elektronikus aláírásban vagy az elektronikus dokumentumkonténerben; és

c) igazolniuk kell a fokozott biztonságú elektronikus aláírás hitelességét, amennyiben:

1. a fokozott biztonságú elektronikus aláírást alátámasztó tanúsítvány érvényes volt az aláírás időpontjában, és ha a fokozott biztonságú elektronikus aláírást minősített tanúsítvány támasztja alá, akkor a fokozott biztonságú elektronikus aláírást alátámasztó minősített tanúsítvány az aláírás időpontjában egy olyan, elektronikus aláírásokra vonatkozó minősített tanúsítvány volt, amely megfelel a 910/2014/EU rendelet I. mellékletének, és egy minősített bizalmi szolgáltató adta ki azt;

2. az aláírás-hitelesítési adatok megfelelnek a szolgáltatást igénybe vevő fél számára megadott adatoknak;

3. a szolgáltatást igénybe vevő fél pontosan megkapja az aláírót egyedi módon azonosító adatokat;

4. amennyiben az aláírás időpontjában álnév használatára került sor, az álnév használatának tényét egyértelműen feltüntették a szolgáltatást igénybe vevő fél számára;

5. ha a fokozott biztonságú elektronikus aláírást minősített elektronikus aláírást létrehozó eszközzel állítottak elő, bármely ilyen eszköz használatát egyértelműen feltüntették a szolgáltatást igénybe vevő fél számára;

6. az aláírt adatok sértetlensége nem került veszélybe;

7. az aláírás időpontjában teljesültek a 910/2014/EU rendelet 26. cikkében foglalt követelmények;

8. a fokozott biztonságú elektronikus aláírás hitelesítésére használt rendszer biztosítja a hitelesítési eljárás pontos eredményét a szolgáltatást igénybe vevő fél számára, és lehetővé teszi, hogy a szolgáltatást igénybe vevő fél minden, a biztonságot érintő problémát észleljen.

3. cikk

A 910/2014/EU rendelet 37. cikkének (1) és (2) bekezdése szerint fokozott biztonságú elektronikus bélyegzőt vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegzőt előíró tagállamok elismerik az XML, CMS és PDF formátumú, B, T vagy LT megfelelőségi szintű fokozott biztonságú elektronikus bélyegzőket, valamint a kapcsolódó aláírás-konténert tartalmazó fokozott biztonságú elektronikus bélyegzőket, amennyiben a bélyegzők megfelelnek a mellékletben foglalt technikai specifikációnak.

4. cikk

(1) A 910/2014/EU rendelet 37. cikkének (1) és (2) bekezdése szerint fokozott biztonságú elektronikus bélyegzőt vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegzőt előíró tagállamok elismerik az e határozat 3. cikkében említett elektronikus bélyegzőformátumoktól eltérő formátumokat is, feltéve, hogy a bélyegző létrehozója által igénybe vett bizalmi szolgáltató székhelye szerinti tagállam más tagállamoknak bélyegzőhitelesítési lehetőségeket kínál, amelyek lehetőség szerint alkalmasak automatizált feldolgozásra.

(2) A bélyegzőhitelesítési lehetőségeknek:

a) lehetővé kell tenniük a tagállamok számára, hogy online, ingyenesen és a nyelvet nem beszélők számára is érthetően hitelesítsék a kapott elektronikus bélyegzőket;

b) meg kell jelenniük a bélyegzővel ellátott dokumentumban, az elektronikus bélyegzőben vagy az elektronikus dokumentumkonténerben;

c) igazolniuk kell a fokozott biztonságú elektronikus bélyegző hitelességét, amennyiben:

1. a fokozott biztonságú elektronikus bélyegzőt alátámasztó tanúsítvány érvényes volt a bélyegzés időpontjában, és ha a fokozott biztonságú elektronikus bélyegzőt minősített tanúsítvány támasztja alá, akkor a fokozott biztonságú elektronikus bélyegzőt alátámasztó minősített tanúsítvány a bélyegzés időpontjában egy olyan, elektronikus bélyegzőkre vonatkozó minősített tanúsítvány volt, amely megfelel a 910/2014/EU rendelet III. mellékletének, és egy minősített bizalmi szolgáltató adta ki azt;

2. a bélyegzőhitelesítési adatok megfelelnek a szolgáltatást igénybe vevő fél számára megadott adatoknak;

3. a szolgáltatást igénybe vevő fél pontosan megkapja a bélyegző létrehozóját egyedi módon azonosító adatokat;

4. amennyiben a bélyegzés időpontjában álnév használatára került sor, az álnév használatának tényét egyértelműen feltüntették a szolgáltatást igénybe vevő fél számára;

5. ha a fokozott biztonságú elektronikus bélyegzőt minősített elektronikus bélyegzőt létrehozó eszközzel állítottak elő, bármely ilyen eszköz használatát egyértelműen feltüntették a szolgáltatást igénybe vevő fél számára;

6. a bélyegzővel ellátott adatok sértetlensége nem került veszélybe;

7. a bélyegzés időpontjában teljesültek a 910/2014/EU rendelet 36. cikkében foglalt követelmények;

8. a fokozott biztonságú elektronikus bélyegző hitelesítésére használt rendszer biztosítja a hitelesítési eljárás pontos eredményét a szolgáltatást igénybe vevő fél számára, és lehetővé teszi, hogy a szolgáltatást igénybe vevő fél minden, a biztonságot érintő problémát észleljen.

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

MELLÉKLET

Az XML, CMS és PDF formátumú, fokozott biztonságú elektronikus aláírásokra és a kapcsolódó aláírás-konténerre vonatkozó technikai specifikációk jegyzéke

A határozat 1. cikkében említett fokozott biztonságú elektronikus aláírásoknak meg kell felelniük az alábbi ETSI technikai specifikációk egyikének, kivéve azok 9. pontját:

XAdES alapprofil	ETSI TS 103171 v.2.1.1. ([1])
CAdES alapprofil	ETSI TS 103173 v.2.2.1. ([2])
PAdES alapprofil	ETSI TS 103172 v.2.2.2. ([3])

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf
([2]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf
([3]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

A határozat 1. cikkében említett kapcsolódó aláírás-konténernek meg kell felelnie az alábbi ETSI technikai specifikációnak:

A kapcsolódó aláírás-konténer alapprofilja	ETSI TS 103174 v.2.2.1 ([1])

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf

Az XML, CMS és PDF formátumú, fokozott biztonságú elektronikus bélyegzőkre és a kapcsolódó bélyegzőkonténerre vonatkozó technikai specifikációk jegyzéke

A határozat 3. cikkében említett fokozott biztonságú elektronikus bélyegzőknek meg kell felelniük az alábbi ETSI technikai specifikációk egyikének, kivéve azok 9. pontját:

XAdES alapprofil	ETSI TS 103171 v.2.1.1.
CAdES alapprofil	ETSI TS 103173 v.2.2.1.
PAdES alapprofil	ETSI TS 103172 v.2.2.2.

A határozat 3. cikkében említett kapcsolódó bélyegzőkonténernek meg kell felelnie az alábbi ETSI technikai specifikációnak:

A kapcsolódó bélyegzőkonténer alapprofilja	ETSI TS 103174 v.2.2.1.

ISSN 1977-0731 (elektronikus kiadás)
ISSN 1725-5090 (nyomtatott kiadás)

Az Európai Unió Kiadóhivatala
2985 Luxembourg
LUXEMBURG

HU