Ez a dokumentum kizárólag tájékoztató jellegű, az intézmények semmiféle felelősséget nem vállalnak a tartalmáért

►B ►C1 **A BIZOTTSÁG HATÁROZATA**

(2009. október 16.)

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

(az értesítés a C(2009) 7806. számú dokumentummal történt)

(EGT-vonatkozású szöveg)

(2009/767/EK) ◄

(HL L 274., 2009.10.20., 36. o.)

Módosította:

		Hivatalos Lap		
		Szám	Oldal	Dátum
►M1	A Bizottság 2010/425/EU határozata (2010. július 28.)	L 199	30	2010.7.31.

Helyesbítette:

►C1 Helyesbítés, HL L 299., 2009.11.14., 18. o. (2009/767/EK)
►C2 Helyesbítés, HL L 4., 2011.1.7., 6. o. (2009/767/EK)

▼B
▼C1

A BIZOTTSÁG HATÁROZATA

(2009. október 16.)

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

(az értesítés a C(2009) 7806. számú dokumentummal történt)

(EGT-vonatkozású szöveg)

(2009/767/EK)

AZ EURÓPAI KÖZÖSSÉGEK BIZOTTSÁGA,

tekintettel az Európai Közösséget létrehozó szerződésre,

tekintettel a belső piaci szolgáltatásokról szóló, 2006. december 12-i 2006/123/EK európai parlamenti és tanácsi irányelvre [1] és különösen annak 8. cikke (3) bekezdésére,

mivel:

(1) A 2006/123/EK irányelv II. fejezetében és különösen 5. és 8. cikkében a tagállamok számára előírt igazgatási egyszerűsítés körébe tartozik az a kötelezettség, hogy egyszerűsíteniük kell a szolgáltatási tevékenység nyújtására való jogosultsággal, valamint a szolgáltatási tevékenység gyakorlásával kapcsolatos eljárásokat és alaki követelményeket, valamint annak biztosítási kötelezettsége, hogy ezek az eljárások és alaki követelmények távolról, elektronikus úton az egyablakos ügyintézési pontokon keresztül egyszerűen teljesíthetőek legyenek.

(2) A 2006/123/EK irányelv 8. cikkében foglaltak szerint az eljárások és alaki követelmények egyablakos ügyintézési pontokon keresztül történő teljesítését a tagállamok határain átnyúlóan is biztosítani kell.

(3) Az eljárások és alaki követelmények egyszerűsítésére vonatkozó kötelezettség teljesítése, valamint az egyablakos ügyintézési pontok határokon átnyúló használatának lehetővé tétele céljából az elektronikus eljárásoknak egyszerű megoldásokra kell alapulniuk, ideértve az elektronikus aláírás használatát is. Olyan esetekben, amikor az adott eljárások és alaki követelmények megfelelő kockázatértékelését követően magas fokú biztonságot vagy a kézi aláírással egyenértékű megoldást tartanak szükségesnek, minősített tanúsítványon alapuló – biztonságos aláírás-létrehozó eszközzel vagy anélkül létrehozott –, a szolgáltatóktól egyes eljárások és alaki követelmények tekintetében minősített tanúsítványon alapuló – biztonságos aláírás-létrehozó eszközzel vagy anélkül létrehozott –, fokozott biztonságú elektronikus aláírás követelhető meg.

[1] HL L 376., 2006.12.27., 36. o.

▼C1

(4) Az elektronikus aláírás közösségi keretrendszerét az elektronikus aláírásra vonatkozó közösségi keretfeltételekről szóló, 1999. december 13-i 1999/93/EK európai parlamenti és tanácsi irányelv ([1]) hozta létre. A minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírások határokon átnyúló használatának megkönnyítése érdekében fokozni kell az ilyen elektronikus aláírásokba vetett bizalmat, tekintet nélkül arra, hogy az aláíró vagy a minősített tanúsítványt kiállító hitelesítésszolgáltató melyik tagállamban telepedett le. Ez úgy érhető el, hogy az elektronikus aláírás érvényességének ellenőrzéséhez szükséges információkat megbízható formában, könnyebben hozzáférhetővé teszik, ideértve különösen a valamely tagállamban felügyelt/akkreditált hitelesítésszolgáltatókra és az általuk kínált szolgáltatásokra vonatkozó információkat.

(5) Biztosítani kell, hogy a tagállamok ezeket az információkat egységes sablont alkalmazva közzéteszik az információk használhatóságának és annak biztosítása érdekében, hogy az információk kellően részletesek ahhoz, hogy a fogadó oldal az elektronikus aláírás érvényességét ellenőrizhesse,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

Az elektronikus aláírások használata és elfogadása

(1) Ha az a kockázatok megfelelő értékelése alapján indokolt, illetve a 2006/123/EK irányelv 5. cikke (1) és (3) bekezdésének megfelelően a tagállamok egyes eljárásoknak és alaki követelményeknek a 2006/123/EK irányelv 8. cikke szerinti egyablakos ügyintézési helyeken keresztül történő teljesítése érdekében megkövetelhetik, hogy a szolgáltató minősített tanúsítványon alapuló – biztonságos aláírás-létrehozó eszközzel vagy anélkül létrehozott –, fokozott biztonságú, az 1999/93/EK irányelvben meghatározott elektronikus aláírást használjon, amely aláírásra ez utóbbi irányelvet kell alkalmazni.

(2) A tagállamoknak az (1) bekezdésben említett eljárások és alaki követelmények teljesítéséhez a minősített tanúsítványon alapuló és biztonságos aláírás-létrehozó eszközzel vagy anélkül létrehozott valamennyi, fokozott biztonságú elektronikus aláírást el kell fogadniuk, a tagállamok számára nyitva álló azon lehetőség sérelme nélkül, hogy az elfogadást a minősített tanúsítványon alapuló és biztonságos aláírás-létrehozó eszközzel létrehozott, fokozott biztonságú elektronikus aláírásra korlátozzák, ha az (1) bekezdésben említett kockázatértékeléssel ez összhangban áll.

(3) A tagállamok a minősített tanúsítványon alapuló, biztonságos aláírás-létrehozó eszközzel vagy anélkül létrehozott, fokozott biztonságú elektronikus aláírás elfogadását nem köthetik olyan feltételekhez, amelyek akadályt jelentenek az eljárásoknak a szolgáltatók által elektronikus úton, az egyablakos ügyintézési helyeken keresztül történő teljesítése előtt.

([1]) HL L 13., 2000.1.19., 12. o.

▼C1

(4) A (2) bekezdés ellenére a tagállamok a minősített tanúsítványon alapuló és biztonságos aláírás-létrehozó eszközzel vagy anélkül létrehozott, fokozott biztonságú elektronikus aláírástól eltérő elektronikus aláírást is elfogadhatnak.

2. cikk

A megbízható szolgáltatók listájának létrehozása, vezetése és közzététele

(1) A tagállamok – a mellékletben meghatározott technikai leírásnak megfelelően – létrehozzák, vezetik és közzéteszik a megbízható szolgáltatók listáját, amely a tagállam által felügyelt/akkreditált, a nyilvánosság számára minősített tanúsítványokat kiállító hitelesítésszolgáltatókra vonatkozó minimálisan előírt adatokat tartalmazza.

▼M1

(2) A tagállamok a megbízható szolgáltatóknak a mellékletben meghatározott műszaki leírásnak megfelelő listáját mind emberi szemmel olvasható, mind géppel feldolgozható formátumban létrehozzák és közzéteszik.

(2a) A tagállamok a megbízható szolgáltatók listájának géppel feldolgozható formátumát elektronikus aláírással látják el, és a megbízható szolgáltatók listáját – annak eredetisége és integritása igazolásának érdekében – legalább emberi szemmel olvasható formátumban, biztonságos csatornán keresztül közzéteszik.

(3) A tagállamok bejelentik a Bizottságnak a következő adatokat:

a) a megbízható szolgáltatók listája emberi szemmel olvasható és géppel feldolgozható formátumának létrehozásáért, vezetéséért és közzétételéért felelős szervezet vagy szervezetek nevét;

b) a megbízható szolgáltatók listája emberi szemmel olvasható és géppel feldolgozható formátumának közzétételi helyét;

c) az azon biztonságos csatorna implementációjához használt nyilvánoskulcs-tanúsítványt, amelyen keresztül a megbízható szolgáltatók listájának emberi szemmel olvasható formátumát közzéteszik, vagy ha az emberi szemmel olvasható listát elektronikus aláírással látták el, akkor az annak aláírásához használt nyilvánoskulcs-tanúsítványt;

d) a megbízható szolgáltatók géppel feldolgozható listájának elektronikus aláírásához használt nyilvánoskulcs-tanúsítványt;

e) az a)–d) pontban említett adatokkal kapcsolatos minden változást.

(4) A Bizottság a tagállamok által bejelentett, a (3) bekezdésben említett adatokat emberi szemmel olvasható és aláírt, valamint géppel feldolgozható formátumban is valamennyi tagállam rendelkezésére bocsátja hitelesített webszerverre mutató biztonságos csatornán keresztül.

▼C1

3. cikk

Alkalmazás

Ezt a határozatot 2009. december 28-tól kell alkalmazni.

4. cikk

Címzettek

Ennek a határozatnak a tagállamok a címzettjei.

▼C1

MELLÉKLET

A „FELÜGYELT/AKKREDITÁLT MEGBÍZHATÓ HITELESÍTÉSSZOLGÁLTATÓK LISTÁJA” EGYSÉGES SABLONJÁNAK TECHNIKAI LEÍRÁSA

ELŐSZÓ

1. **Általános rész**

A „Felügyelt/akkreditált megbízható hitelesítésszolgáltatók listájának” tagállamok részére szóló egységes sablonja azzal a céllal készült, hogy egységes módszert állapítson meg az egyes tagállamok számára az általuk az 1999/93/EK irányelv vonatkozó rendelkezéseinek megfelelően felügyelt/akkreditált hitelesítésszolgáltatóktól ([1]) származó hitelesítési szolgáltatások felügyeleti/akkreditációs státusára vonatkozó adatok megadására. Ebbe a körbe beletartoznak a felügyelt/akkreditált hitelesítési szolgáltatások felügyeleti/akkreditációs státusának előzményeire vonatkozó adatok is.

A hitelesített szolgáltatók listájában szereplő kötelező információk között szerepelnie kell a minősített tanúsítványokat ([2]) kiállító, az 1999/93/EK irányelv rendelkezéseiben (a 3. cikk (3) bekezdése, a 3. cikk (2) bekezdése és a 7. cikk (1) bekezdésének a) pontja) foglaltak szerint felügyelt/akkreditált hitelesítésszolgáltatókra vonatkozó minimális adatoknak, ideértve az elektronikus aláírások alapját képező minősített tanúsítványok adatait, és azt is, hogy az aláírás biztonságos aláírás-létrehozó eszközzel vagy anélkül készült ([3]).

A hitelesített szolgáltatók nemzeti listájába önkéntes alapon minősített tanúsítványok kiállításával nem foglalkozó, de elektronikus aláíráshoz kapcsolódó szolgáltatásokat nyújtó (pl. időbélyegző szolgáltatást nyújtó és időbélyeget kiadó hitelesítésszolgáltató, fokozott biztonságú tanúsítványokat kiállító hitelesítésszolgáltató stb.), további felügyelt/akkreditált hitelesítésszolgáltatók is felvehetők.

Ezeknek az adatoknak az elsődleges célja a minősített elektronikus aláírások és a minősített tanúsítvánnyal ellátott fokozott biztonságú elektronikus aláírások ([4]) érvényessége ellenőrzésének támogatása ([5]) ([6]).

A javasolt egységes sablon kompatibilis az ETSI TS 102 231-ben ([7]) meghatározott, az ilyen listák létrehozására, közzétételére, helyére, elérhetőségére, eredetvizsgálatára és hitelesítésére szolgáló tanúsítványprofilokat használó rendszerekkel.

([1]) Az 1999/93/EK irányelv 2. cikkének (11) bekezdésében szereplő fogalommeghatározás szerint.

([2]) Az 1999/93/EK irányelv 2. cikkének (10) bekezdésében szereplő fogalommeghatározás szerint.

([3]) Az 1999/93/EK irányelv 2. cikkének (6) bekezdésében szereplő fogalommeghatározás szerint.

([4]) Az 1999/93/EK irányelv 2. cikkének (2) bekezdésében szereplő fogalommeghatározás szerint.

([5]) Ennek a dokumentumnak az angol nyelvű változatában a minősített tanúsítvánnyal ellátott fokozott biztonságú elektronikus aláírást az „$AdES_{QC}$” rögzítéssel jelöljük.

([6]) Felhívjuk a figyelmet arra, hogy számos elektronikus szolgáltatás alapul egyszerű fokozott biztonságú elektronikus aláírásokon, amelyek határokon átnyúló használatát is lehetővé kell tenni, feltéve, hogy a mögöttes hitelesítési szolgáltatások (melyek pl. fokozott biztonságú tanúsítványokat adnak ki) szerepelnek az adott tagállam megbízható szolgáltatói listájának önkéntes részében.

([7]) ETSI TS 102231 – Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.

▼C1

2. **Iránymutatás a megbízható szolgáltatók listájában található bejegyzések szerkesztéséhez**

2.1. *A megbízható szolgáltatók felügyelt/akkreditált hitelesítési szolgáltatásokon alapuló listája*

A megfelelő hitelesítési szolgáltatások és hitelesítésszolgáltatók egyetlen listában szerepelnek

A tagállam megbízható szolgáltatóinak listája a következőképpen határozható meg: „A tagállam által az 1999/93/EK irányelv vonatkozó rendelkezéseinek betartása tekintetében felügyelt/akkreditált hitelesítésszolgáltatók hitelesítési szolgáltatásainak felügyeleti/akkreditációs státuslistája.”

A megbízható szolgáltatók ilyen listájának a következőket kell tartalmaznia:

— az 1999/93/EK irányelv 2. cikkének (11) bekezdésében meghatározott **valamennyi hitelesítésszolgáltató**, azaz „olyan intézmény, illetve természetes vagy jogi személy, aki, illetve amely tanúsítványokat bocsát ki, vagy egyéb, elektronikus aláírásokhoz kapcsolódó szolgáltatásokat nyújt”,

— **amelyet** az 1999/93/EK irányelvben megállapított, vonatkozó rendelkezések betartása tekintetében **felügyelnek/akkreditáltak**.

Az 1999/93/EK irányelvben – különösen az érintett hitelesítésszolgáltatók és felügyeleti/önkéntes akkreditációs rendszereik vonatkozásában – megállapított fogalommeghatározásokat és rendelkezéseket vizsgálva kétféle hitelesítésszolgáltatót különböztethetünk meg, nevezetesen a nyilvánosságnak minősített tanúsítványt kiállító hitelesítésszolgáltatókat, és a nyilvánosságnak minősített tanúsítvány kiállításával nem foglalkozó olyan hitelesítésszolgáltatókat, amelyek „egyéb, elektronikus aláírásokhoz kapcsolódó (kiegészítő) szolgáltatásokat nyújtanak”:

— **Minősített tanúsítványt kiállító hitelesítésszolgáltatók**

— Ezek felügyeletét a letelepedés helye szerinti tagállam látja el (amennyiben ezek valamely tagállamban telepedtek le), és ezek az 1999/93/EK irányelvben megállapított rendelkezéseknek – ideértve az I. melléklet (A minősített tanúsítványra vonatkozó követelmények) és a II. melléklet (A minősített tanúsítványokat kiállító hitelesítésszolgáltatóra vonatkozó követelmények) követelményeit – való megfelelés tekintetében akkreditálhatóak is. Egy tagállam megfelelő felügyeleti rendszerének az abban akkreditált minősített tanúsítványt kiállító hitelesítésszolgáltatókra is ki kell terjednie, kivéve, ha ezek nem telepedtek le ebben a tagállamban.

— Meghatározták az alkalmazandó „felügyeleti” rendszert (illetve „önkéntes akkreditációs” rendszert), és annak meg kell felelnie az 1999/93/EK irányelvben és különösen annak 3. cikke (3) bekezdésében, 8. cikke (1) bekezdésében, 11. cikkében, (13) preambulumbekezdésében (illetve 2. cikke (13) bekezdésében, 3. cikke (2) bekezdésében, 7. cikke (1) bekezdésének a) pontjában, 8. cikke (1) bekezdésében, 11. cikkében, (4) és (11)–(13) preambulumbekezdésében) megállapított feltételeknek.

— **Minősített tanúsítvány kiállításával nem foglalkozó hitelesítésszolgáltatók**

— Ezek (az 1999/93/EK irányelvben meghatározott és annak megfelelő) „önkéntes akkreditációs” rendszer és/vagy az irányelv rendelkezései – és esetlegesen (az irányelv 2. cikke (11) bekezdésének értelmében vett) hitelesítési szolgáltatások nyújtása tekintetében érvényesülő nemzeti rendelkezések – betartásának felügyeletére az adott országban meghatározott és nemzeti alapon végrehajtott „elismert jóváhagyási rendszer” hatálya alá tartozhatnak.

— A hitelesítési szolgáltatások nyújtásának eredményeként generált vagy kiállított fizikai vagy bináris (logikai) objektumok a nemzeti szinten megállapított rendelkezések és követelmények teljesítése alapján jogosultak lehetnek valamely külön minősítésre, de az ilyen „minősítés” hatálya valószínűleg kizárólag nemzeti szintű.

▼C1

A megbízható szolgáltatók tagállami listájának tartalmaznia kell a minősített tanúsítványokat kiállító, az 1999/93/EK irányelv rendelkezéseiben (a 3. cikk (3) bekezdése, a 3. cikk (2) bekezdése és a 7. cikk (1) bekezdésének a) pontja) megállapítottak szerint felügyelt/akkreditált hitelesítésszolgáltatókra vonatkozó minimális adatokat, az elektronikus aláírások alapját képező minősített tanúsítványokra vonatkozó adatokat, és azt, hogy az aláírás biztonságos aláírás-létrehozó eszközzel vagy anélkül készült.

A hitelesített szolgáltatók nemzeti listájába önkéntes alapon minősített tanúsítványok kiállításával nem foglalkozó, de elektronikus aláíráshoz kapcsolódó szolgáltatásokat nyújtó (pl. időbélyegző szolgáltatást nyújtó és időbélyeget kiadó hitelesítésszolgáltató, fokozott biztonságú tanúsítványokat kiadó hitelesítésszolgáltató stb.), más felügyelt/akkreditált hitelesítésszolgáltatókra vonatkozó további adatok is felvehetők.

A megbízható szolgáltatók listájának célja:

— azon hitelesítésszolgáltatók hitelesítési szolgáltatásainak felügyeleti/akkreditációs státusára vonatkozó adatok nyilvántartása és megadása, amelyeket az 1999/93/EK irányelv vonatkozó rendelkezéseinek betartása tekintetében a listát létrehozó és vezető tagállam felügyel/akkreditál;

— a listán szereplő hitelesítésszolgáltatók listán szereplő, felügyelt/akkreditált hitelesítési szolgáltatásain alapuló elektronikus aláírások érvényessége ellenőrzésének lehetővé tétele.

Egyetlen felügyeleti-/akkreditációsstátusz-értéksorozat

A megbízható szolgáltatókról tagállamonként egy-egy listát kell létrehozni és vezetni, az adott tagállam által felügyelt/akkreditált hitelesítésszolgáltatók hitelesítési szolgáltatásai felügyeleti/akkreditációs státusának feltüntetése érdekében.

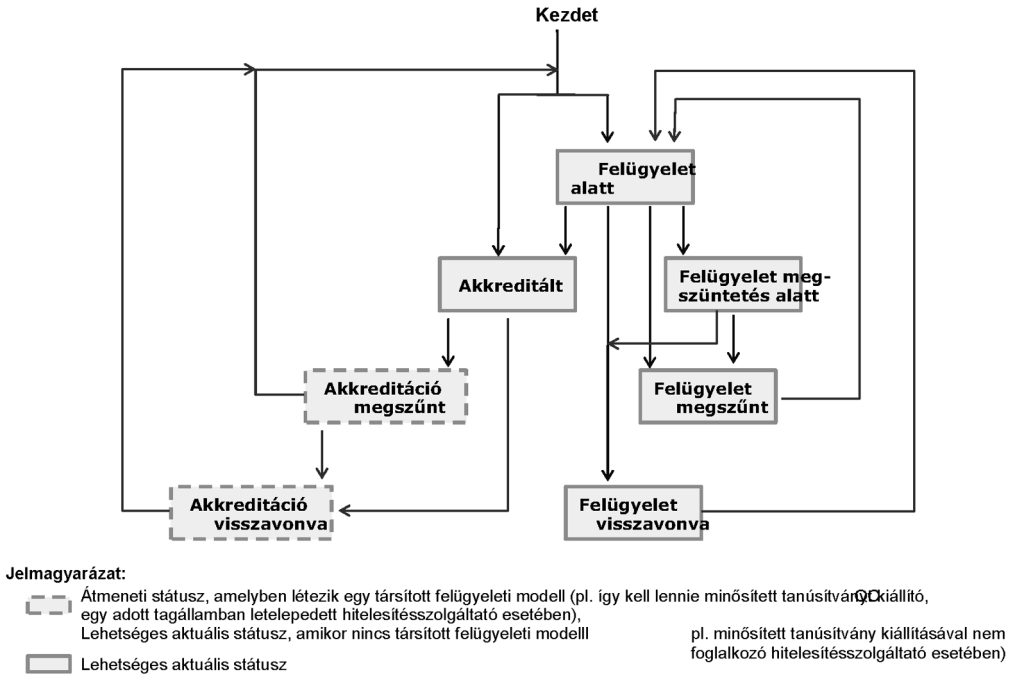
Az a tény, hogy valamely szolgáltatás felügyelet alatt áll vagy akkreditált, hozzátartozik az aktuális státushoz. Emellett a felügyeleti/akkreditációs státus lehet „folyamatos”, „megszüntetés alatt”, „megszűnt” vagy akár „visszavont”. Valamely hitelesítési szolgáltatás élettartama alatt felügyeleti státusról akkreditációs státusra is áttérhet és viszont ([1]).

Az alábbi 1. ábra egyetlen hitelesítési szolgáltatás lehetséges felügyeleti/akkreditációs státusok közötti várható mozgását ábrázolja:

([1]) Pl. egy tagállamban letelepedett hitelesítésszolgáltató, amely valamely, eredetileg a tagállam (felügyeleti szerv) által felügyelt hitelesítési szolgáltatást nyújt, bizonyos idő elteltével határozhat úgy, hogy a jelenleg felügyelt hitelesítési szolgáltatás tekintetében akkreditációt kér. Megfordítva: egy másik tagállamban lévő hitelesítésszolgáltató határozhat úgy, hogy nem hagy fel az akkreditált hitelesítési szolgáltatással, hanem – pl. üzleti és/vagy gazdasági okokból – az akkreditációs státusról áttér a felügyeleti státusra.

▼C1

Egy adott hitelesítési szolgáltatás felügyeleti / akkreditációs státuszának lehetséges változásai



1. ábra

A minősített tanúsítványt kiállító hitelesítésszolgáltatónak felügyelet alatt kell állnia (ha valamely tagállamban letelepedett), és önkéntes akkreditációval is rendelkezhet. A megbízható szolgáltatók listájában szereplő szolgáltatás státusértéke a fent „aktuális státusértékként” megjelölt értékek bármelyike lehet. Meg kell azonban jegyezni, hogy az „Akkreditáció megszűnt” és az „Akkreditáció visszavonva” értéknek csak a valamely tagállamban letelepedett, minősített tanúsítványt kiállító hitelesítésszolgáltatók szolgáltatásai esetében kell átmeneti értéknek lennie, hiszen ezek a szolgáltatások alapértelmezésben (akkreditáció nélkül vagy annak megszűnése esetén is) felügyelet alatt állnak.

Előírás, hogy azoknak a tagállamoknak, amelyek a minősített tanúsítvány kiállításával nem foglalkozó hitelesítésszolgáltatók szolgáltatásainak az 1999/93/EK irányelvben megállapított rendelkezések és (az irányelv 2. cikke (11) bekezdésének értelmében vett) hitelesítési szolgáltatások nyújtása tekintetében érvényesülő nemzeti rendelkezések betartásának felügyeletére az adott országban meghatározott és nemzeti alapon végrehajtott „elismert jóváhagyási rendszert” hoztak vagy hoznak létre, az ilyen jóváhagyási rendszereket az alábbi két kategória egyikébe kell besorolniuk:

— „önkéntes akkreditáció”, az 1999/93/EK irányelvben (annak 2. cikke (13) bekezdésében, 3. cikke (2) bekezdésében, 7. cikke (1) bekezdésének a) pontjában, 8. cikke (1) bekezdésében, 11. cikkében, (4) és (11)–(13) preambulumbekezdésében) meghatározottak és szabályozottak szerint,

— az 1999/93/EK irányelvben előírt „felügyelet”, a nemzeti jogszabályoknak megfelelő nemzeti rendelkezések és követelmények útján végrehajtva.

▼C1

Ennek megfelelően a minősített tanúsítvány kiállításával nem foglalkozó hitelesítésszolgáltató állhat felügyelet alatt és nem kérhet önkéntes akkreditációt. A megbízható szolgáltatók listájában szereplő ilyen szolgáltatás státusértéke a fent „aktuális státusértékként" megjelölt értékek bármelyike lehet (lásd az 1. ábrát).

A megbízható szolgáltatók listájának tartalmaznia kell az alkalmazott felügyeleti/akkreditációs rendszerekre vonatkozó adatokat, különösen az alábbiakat:

— a minősített tanúsítványt kiállító hitelesítésszolgáltatókra vonatkozó felügyeleti rendszer adatai,

— adott esetben a minősített tanúsítványt kiállító hitelesítésszolgáltatókra vonatkozó nemzeti „önkéntes akkreditációs" rendszer adatai,

— adott esetben a minősített tanúsítvány kiállításával nem foglalkozó hitelesítésszolgáltatókra vonatkozó felügyeleti rendszer adatai,

— Adott esetben a minősített tanúsítvány kiállításával nem foglalkozó hitelesítésszolgáltatókra vonatkozó nemzeti „önkéntes akkreditációs" rendszer adatai.

Az utolsó két adatkészlet kulcsfontosságú a listát használók számára a nemzeti szinten a minősített tanúsítvány kiállításával nem foglalkozó hitelesítésszolgáltatókra alkalmazott felügyeleti/akkreditációs rendszerek minőségének és biztonsági szintjének értékeléséhez. Amennyiben a megbízható szolgáltatók listája tartalmazza a minősített tanúsítvány kiállításával nem foglalkozó hitelesítésszolgáltatókra vonatkozó felügyeleti/akkreditációs státusadatokat, a korábban említett adatkészletet a megbízható szolgáltatók listája szintjén kell megadni, a „Scheme information URI" (a rendszer adatainak URI-ja) (5.3.7. pont – a tagállamok által megadott információk), a „Scheme type/community/rules" (rendszertípus/közösség/szabályok) (5.3.9. pont – a valamennyi tagállam esetében azonos szöveggel és a tagállam által megadott, nem kötelező adatok révén) és a „TSL policy/legal notice" (megbízható állapotlista szabályzata/jogi figyelmeztetés) (5.3.11. pont – a valamennyi tagállam esetében azonos, az 1999/93/EK irányelvre utaló szöveg, azzal, hogy minden tagállam feltüntetheti a tagállamra jellemző egyedi szöveget/hivatkozásokat) mezők használatával. Adott esetben a minősített tanúsítvány kiállításával nem foglalkozó hitelesítésszolgáltatókra vonatkozó nemzeti felügyeleti/akkreditációs rendszerek szintjén meghatározott, további, „minősítésre" vonatkozó adatokat szükség esetén (pl. több minőségi/biztonsági szint megkülönböztetése érdekében) szolgáltatási szinten lehet megadni a „Service information extension" (szolgáltatásinformáció-bővítmény) (5.5.9. pont) részét képező „additionalServiceInformation" (szolgáltatás további adatai) bővítmény (5.8.2. pont) használatával. A vonatkozó műszaki leírásra vonatkozó további információk az I. fejezetben található részletes leírásban olvashatóak.

Habár a tagállamban a tagállam hitelesítési szolgáltatásainak felügyelete és akkreditációja több szervnek is feladata lehet, elvárás, hogy egy hitelesítési szolgáltatást (amelyet az ETSI TS 102231 szerint a „Service digital identity" [szolgáltatás digitális azonosítója] azonosít [1]) a listába csak egyszer vigyenek fel, és felügyeleti/akkreditációs státusát megfelelően frissítsék. A fent megjelölt státusok jelentését az I. fejezetben található részletes műszaki leírás 5.5.4. pontja ismerteti.

2.2. *A megbízható szolgáltatók listájában a minősített elektronikus aláírások és a minősített tanúsítvánnyal ellátott fokozott biztonságú elektronikus aláírások érvényességének ellenőrzését elősegítő bejegyzések*

A megbízható szolgáltatók listája létrehozásának legnagyobb jelentőségű része a lista kötelező részének kialakítása, nevezetesen a minősített tanúsítványt kiállító hitelesítésszolgáltatók esetében a „List of services" (a szolgáltatások listája) mező létrehozása annak érdekében, hogy az minden kiállított minősített tanúsítvány esetében megfelelően mutassa a minősített tanúsítványt kiállító hitelesítésszolgáltató pontos státusát, valamint hogy biztosítsa, hogy az egyes bejegyzésekben feltüntetett adatok elegendőek legyenek a minősített elektronikus aláírás és (ha azt a hitelesítésszolgáltató a bejegyzésben szereplő hitelesítési szolgáltatás keretében a végfelhasználói minősített tanúsítvány tartalmával kombinálja) a minősített tanúsítvánnyal ellátott fokozott biztonságú elektronikus aláírás érvényességének ellenőrzéséhez.

[1] ETSI TS 102 231- Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information

▼C1

Amennyiben nem létezik valódi átjárhatóságot biztosító és határokon átnyúló minősített tanúsítványprofil, a szükséges adatok körébe az egyedüli legfelső szintű hitelesítésszolgáltató digitális szolgáltatásazonosítóján („Service digital identity”) túlmenően más adatok is beletartozhatnak, így különösen a kiállított minősített tanúsítvány státusát azonosító adatok, valamint az, hogy a támogatott aláírásokat biztonságos aláírás-létrehozó eszközzel hozták-e létre. A tagállamban a megbízható szolgáltatók listájának létrehozásával, szerkesztésével és vezetésével megbízott szervezetnek (pl. az ETSI TS 102231 szerinti rendszerüzemeltető) ezért a megbízható szolgáltatók listáján szereplő egyes minősített tanúsítványt kiállító hitelesítésszolgáltatók esetében minden egyes kiállított minősített tanúsítvány aktuális profilját és a tanúsítvány tartalmát is figyelembe kell vennie.

Ideális esetben minden egyes kiállított minősített tanúsítványnak – amennyiben azt minősített tanúsítványként tüntetik fel – tartalmaznia kell az ETSI által meghatározott, a minősített tanúsítvány megfelelőségére vonatkozó nyilatkozatot ([1]), valamint – ha azt elektronikus aláírások készítésére szolgáló, biztonságos aláírás-létrehozó eszközzel készültként tüntetik fel – tartalmaznia kell az ETSI által meghatározott biztonságos aláírás-létrehozó eszközön alapuló minősített tanúsítványra vonatkozó nyilatkozatot, és/vagy azt, hogy minden egyes kiállított minősített tanúsítvány tartalmazza az ETSI TS 101 456-ban ([2]) meghatározott QCP/QCP + hitelesítési rend objektumazonosítót (OID-t). A jelenleg kiállított minősített tanúsítványok tartalmi eltérései miatt (pl. az ETSI által meghatározott minősített tanúsítványra vonatkozó nyilatkozat eshetőleges használata) – amelynek oka a minősített tanúsítványt kiállító hitelesítésszolgáltatók részéről különböző szabványok hivatkozásként való használata, e szabványok egyedi értelmezésének jelentős elterjedtsége, illetve a kötelező műszaki leírás vagy szabványok létezése ismeretének hiánya – a fogadó oldal nem hagyatkozhat pusztán az aláíró tanúsítványára (és a társult tanúsítványláncra/elérési útra) annak legalább géppel olvasható formában történő megállapításához, hogy az elektronikus aláírás alapját képező tanúsítvány vajon minősített tanúsítvány-e, és azt az elektronikus aláírás készítéséhez használt biztonságos aláírás-létrehozó eszközzel társították-e az aláíráshoz.

A „Service type identifier” („Sti” – szolgáltatástípus-azonosító), a „Service name” („Sn”- szolgáltatás neve) és a „Service digital identity” („Sdi” – szolgáltatás digitális azonosítója) ([3]) mezőknek a „Service information extensions” („Sie” – szolgáltatásinformáció-bővítmény) mező adataival való kitöltése lehetővé teszi, hogy a megbízható szolgáltatók listájához javasolt egységes sablon teljeskörűen meghatározza a listán szereplő, minősített tanúsítványt kiállító hitelesítésszolgáltató hitelesítési szolgáltatása által kiállított minősített tanúsítvány típusát, és adatokat tudjon szolgáltatni arról, hogy az biztonságos vagy más aláírás-létrehozó eszközön alapul-e (amennyiben ez az adat a kiállított minősített tanúsítványban nem szerepel). Ehhez a bejegyzéshez természetesen külön „Service current status” („Scs” – szolgáltatás aktuális státusa) adat is társul. Ezt az alábbi 2. ábrán szemléltetjük.

Valamely szolgáltatásnak a listán csak a legfelső szintű hitelesítésszolgáltató „Sdi”-jével való feltüntetése annyit jelent, hogy biztosított (a minősített tanúsítványt kiállító hitelesítésszolgáltató, de a hitelesítésszolgáltató felügyeletét ellátó felügyeleti/akkreditáló szerv révén is) az, hogy a legfelső szintű hitelesítésszolgáltató (hierarchia) alatt kiállított végfelhasználói tanúsítvány elegendő, az ETSI által meghatározott és géppel olvasható adatot tartalmaz annak értékeléséhez, hogy a tanúsítvány minősített tanúsítvány-e, és az biztonságos aláírás-létrehozó eszközön alapul-e. Abban az esetben, ha például ez utóbbi állítás nem igaz (pl. a minősített tanúsítványban nem szerepel ETSI szabványnak megfelelő, géppel feldolgozható jelölés arra vonatkozóan, hogy a tanúsítvány alapja biztonságos aláírás-létrehozó eszköz), az adott legfelső szintű hitelesítésszolgáltatónak mindössze az „Sdi” listában való feltüntetése esetén csak az feltételezhető, hogy a legfelső szintű hitelesítésszolgáltatói hierarciában kiállított minősített tanúsítvány nem biztonságos aláírás-létrehozó eszközön alapul. Annak érdekében, hogy ezek a minősített tanúsítványok biztonságos aláírás-létrehozó eszközön alapulónak minősüljenek, e tény feltüntetéséhez a „Sie” mezőt is használni kell (ez azt is jelzi, hogy a minősítés tényét a minősített tanúsítványt kiállító hitelesítésszolgáltató és a felügyeleti vagy akkreditáló szerv is garantálja).

([1]) Lásd: ETSI TS 101 862- Electronic Signatures and Infrastructures (ESI): Qualified Certificate Profile.

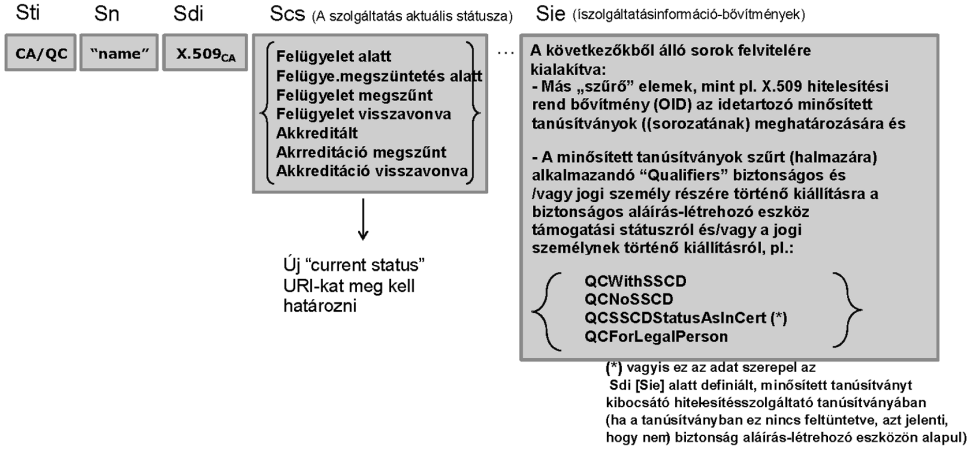
([2]) ETSI TS 101456 – Elektronikus aláírások és infrastruktúrák (ESI). Minősített tanúsítványokat kibocsátó hitelesítésszolgáltatókra vonatkozó szabályzatok követelményei.

([3]) Pl. és legalább az elérési útvonalban a minősített tanúsítványokat kiállító tanúsítványkiállító vagy egy felettes tanúsítványkiállító X.509 v3 tanúsítványának megadása.

▼C1

Általános elvek — Szerkesztési szabályok — Minősített tanúsítványt kiállító hitelesítésszolgáltatók mezői (minősített szolgáltatások)

Szolgáltatások minősített tanúsítványt kiállító hitelesítésszolgáltatók esetén:



2. ábra

A minősített tanúsítványt kiállító hitelesítésszolgáltatók szolgáltatásainak felvitele a megbízható szolgáltatók listájának megbízható szolgáltatások moduljába

A megbízható szolgáltatók listája egységes sablonjának műszaki leírása lehetővé teszi a szolgáltatások felvitelekor az adatok öt fő részének kombinálását:

— a „Service type identifier" („Sti" – szolgáltatástípus-azonosítója), pl. a minősített tanúsítványt kiállító hitelesítésszolgáltató azonosítására („CA/QC"),

— a „Service name" („Sn" – szolgáltatás neve),

— a listába felvett szolgáltatást azonosító „Service digital identity" („Sdi" – szolgáltatás digitális azonosítója) adat, pl. (minimálisan) a minősített tanúsítványt kiállító hitelesítésszolgáltató X.509v3 tanúsítványa,

— a minősített tanúsítványkiállítási szolgáltatások esetében a nem kötelező „Service information extensions" („Sie" – szolgáltatásadat-bővítmény) adat, mely lehetővé teszi egy vagy több olyan értéksor felvitelét, melyek mindegyike megadja az alábbiakat:

  — kritériumok, melyeket az „Sdi"-vel azonosított hitelesítési szolgáltatáson belüli olyan adott szolgáltatások (pl. minősített tanúsítványok csoportja) további azonosítására (szűrésére) használnak, amelyek esetében további adatok szükségesek/állnak rendelkezésre abban a tekintetben, hogy azok biztonságos aláírás-létrehozó eszközön alapulnak-e (és/vagy azokat jogi személy részére állították-e ki), és

  — az arra vonatkozó társított adatok („qualifiers" – minősítők), hogy ez a tovább szűkített szolgáltatáscsoport biztonságos vagy más aláírás-létrehozó eszközön alapul-e, illetve hogy ez a társított adat részét a minősített tanúsítványnak szabványos géppel feldolgozható formában képezi-e, és/-vagy az azt a tényt jelző adat, hogy az ilyen minősített tanúsítványt jogi személy részére állították-e ki (alapértelmezésben a tanúsítványok természetes személy részére kiállítottnak minősülnek).

▼C1

— a szolgáltatásbejegyzés „current status” (aktuális státus) adata, mely a következőkről ad tájékoztatást:

  — hogy a szolgáltatás felügyelt vagy akkreditált-e, és

  — maga a felügyeleti/akkreditációs státus.

2.3. *Szerkesztési és használati iránymutatás a minősített tanúsítványt kiállító hitelesítésszolgáltatók szolgáltatásbejegyzéseihez*

Az **általános szerkesztési szabályok** a következők:

1. Ha biztosított (a minősített tanúsítványt kiállító hitelesítésszolgáltató által adott garancia és a felügyeleti szerv/akkreditáló szerv részéről történő felügyelet/akkreditáció révén) az, hogy az „Sdi”-vel azonosított, a listán szereplő szolgáltatás esetében minden minősített tanúsítvány biztonságos aláírás-létrehozó eszközön alapul, és azokban nem szerepel az ETSI által meghatározott, a minősített tanúsítvány megfelelőségére vonatkozó nyilatkozat, illetve az ETSI által meghatározott, biztonságos aláírás-létrehozó eszközön alapuló minősített tanúsítványra vonatkozó nyilatkozat és/vagy a QCP + objektumazonosító, elegendő a megfelelő „Sdi” mező használata, a „Sie” mező használata pedig opcionális, és abban nem kell arra vonatkozó adatnak szerepelnie, hogy a tanúsítvány biztonságos aláírás-létrehozó eszközön alapul-e.

2. Ha biztosított (a minősített tanúsítványt kiállító hitelesítésszolgáltató által adott garancia és a felügyeleti szerv/akkreditáló szerv részéről történő felügyelet/akkreditáció révén) az, hogy az „Sdi”-vel azonosított, a listán szereplő szolgáltatás esetében az ETSI által meghatározott, a minősített tanúsítvány megfelelőségére vonatkozó nyilatkozat és/vagy a QCP + objektumazonosító a nem biztonságos aláírás-létrehozó eszközön alapuló minden minősített tanúsítványban szerepel, elegendő a megfelelő „Sdi” mező használata, a „Sie” mező használata pedig opcionális, és abban nem kell arra vonatkozó adatnak szerepelnie, hogy a tanúsítvány biztonságos aláírás-létrehozó eszközön alapul (ami annyit jelent, hogy a tanúsítvány nem alapul biztonságos aláírás-létrehozó eszközön.

3. Ha biztosított (a minősített tanúsítványt kiállító hitelesítésszolgáltató által adott garancia és a felügyeleti szerv/akkreditáló szerv részéről történő felügyelet/akkreditáció révén) az, hogy az „Sdi”-vel azonosított, a listán szereplő szolgáltatás esetében minden minősített tanúsítványban szerepel az ETSI által meghatározott, a minősített tanúsítvány megfelelőségére vonatkozó nyilatkozat és a tanúsítványok közül egyesek biztonságos aláírás-létrehozó eszközön alapulnak, mások pedig nem (ilyen megkülönböztetés magában a minősített tanúsítványban is tehető, pl. a hitelesítésszolgáltató egyedi hitelesítési rend objektumazonosítója vagy más, a hitelesítésszolgáltatóra jellemző adat révén, közvetlenül vagy közvetetten, géppel feldolgozható formában vagy másként), de abban nem szerepel SEM az ETSI által meghatározott, biztonságos aláírás-létrehozó eszközön alapuló minősített tanúsítványra vonatkozó nyilatkozat, SEM a QCP + objektumazonosító, nem feltétlenül elegendő a megfelelő „Sdi” mező használata, ÉS a „Sie” mezőt kell használni azon adat kifejezett megadására, hogy a tanúsítvány biztonságos aláírás-létrehozó eszközön alapul-e, az ide tartozó tanúsítványcsoportok azonosítására használt esetleges adatbővítményekkel együtt. Ehhez valószínűleg az adott „Sdi”-hez különböző „SSCD support information values” (a biztonságos aláírás-létrehozó eszközzel való támogatottságot kifejező értékek) mezőket kell felvenni.

4. Ha biztosított (a minősített tanúsítványt kiállító hitelesítésszolgáltató által adott garancia és a felügyeleti szerv/akkreditáló szerv részéről történő felügyelet/-akkreditáció révén) az, hogy az „Sdi”-vel azonosított, a listán szereplő szolgáltatás esetében egy minősített tanúsítványban sem szerepel az ETSI által meghatározott, a minősített tanúsítvány megfelelőségére vonatkozó nyilatkozat, a QCP objektumazonosító, az ETSI által meghatározott, biztonságos aláírás-létrehozó eszközön alapuló minősített tanúsítványra vonatkozó nyilatkozat vagy a QCP + objektumazonosító, de biztosított, hogy az „Sdi” alapján kiállított végfelhasználói tanúsítványok közül egyesek minősített tanúsítványok és/vagy biztonságos aláírás-létrehozó eszközön alapulnak, mások pedig nem (ilyen megkülönböztetés magában a minősített tanúsítványban is tehető, pl. a hitelesítésszolgáltató egyedi hitelesítési rend objektumazonosítója vagy más, a hitelesítésszolgáltatóra jellemző adat révén, közvetlenül vagy közvetetten, géppel feldolgozható formában vagy másként), nem feltétlenül elegendő a megfelelő „Sdi” mező használata, ÉS a „Sie” mezőt kell használni azon adat kifejezett megadására, hogy a tanúsítvány biztonságos aláírás-létrehozó eszközön alapul-e. Ehhez valószínűleg az adott „Sdi”-hez fel kell venni különböző „SSCD support information values” (a biztonságos aláírás-létrehozó eszközzel való támogatottságot kifejező értékek) mezőket.

▼C1

Általános alapértelmezett elvként a megbízható szolgáltatók listájára felvett hitelesítésszolgáltatók esetében minden egyes X.509v3 tanúsítványhoz egy szolgáltatásbejegyzésnek kell tartoznia a minősített tanúsítványkiállítás típusú hitelesítési szolgáltatás esetén, azaz a minősített tanúsítványt (közvetlenül) kiállító hitelesítésszolgáltató esetében. Egyes körültekintően meghatározott körülmények esetében és gondosan irányított feltételek mellett a tagállami felügyeleti szerv/akkreditáló szerv dönthet a gyökértanúsítvány- vagy felső szintű tanúsítványkiadó (azaz a végfelhasználói tanúsítványok közvetlen kiállításával nem foglalkozó, de a hitelesítésszolgáltatók hierarchiáját a végfelhasználóknak minősített tanúsítványt kiállító tanúsítványkiadók felé hitelesítő szolgáltatók) X.509v3 tanúsítványának a listán szereplő hitelesítésszolgáltató szolgáltatásjegyzékében szereplő egyetlen bejegyzés „Sdi”-jeként történő használata mellett. A tagállamoknak körültekintően mérlegelniük kell és jóvá kell hagyniuk a gyökértanúsítvány- vagy felső szintű tanúsítványkiadó X.509v3 tanúsítványának a megbízható szolgáltató listáján „Sdi” értékként történő használata következményeit (előnyeit vagy hátrányait). Emellett, az alapértelmezett elvtől való ezen engedélyezett kivétel alkalmazásakor a tagállamnak át kell adnia a hitelesítési elérési útvonal felépítését és ellenőrzését lehetővé tevő szükséges dokumentációt.

Az általános szerkesztési iránymutatások szemléltetésére a következő példát említhetjük: azon minősített tanúsítványt kiállító hitelesítésszolgáltatók esetében, amelyek olyan legfelső szintű hitelesítésszolgáltatót használnak, amely alatt több tanúsítványkiadó állít ki minősített és fokozott biztonságú tanúsítványokat, de amelynek esetében a minősített tanúsítványokban csak a minősített tanúsítvány megfelelőségére vonatkozó nyilatkozat szerepel, és az nem tünteti fel, hogy a tanúsítvány biztonságos aláírás-létrehozó eszközön alapul-e, a legfelső szintű hitelesítésszolgáltató „Sdi”-jének listán való feltüntetése csak annyit jelent – a fent kifejtett szabályok értelmében –, hogy az ebben a legfelső szintű hitelesítésszolgáltatói hierarchiában kiállított tanúsítványok nem alapulnak biztonságos aláírás-létrehozó eszközön. Ha ezek a minősített tanúsítványok ténylegesen biztonságos aláírás-létrehozó eszközön alapulnak, nyomatékosan ajánlott a jövőben kiállított minősített tanúsítványokban a biztonságos aláírás-létrehozó eszközön alapuló minősített tanúsítványra vonatkozó nyilatkozat igénybe vétele. Időközben (az ezt az adatot nem tartalmazó utolsó minősített tanúsítvány lejártáig), a megbízható állapotlistának használnia kell a „Sie” mezőt és a társított „Qualifications” (minősítések) bővítményt, azaz a tanúsítványokat a minősített tanúsítványt kiállító hitelesítésszolgáltatók által meghatározott és általuk használható objektumazonosítókra kell szűrnie annak érdekében, hogy meg lehessen különböztetni a minősített tanúsítványok különféle típusait (egyesek biztonságos aláírás-létrehozó eszközön alapulnak, mások pedig nem), és minősítők használata révén kifejezetten meg kell adni az adatot, hogy a tanúsítvány biztonságos aláírás-létrehozó eszközön alapul-e.

A megbízható szolgáltatók listájának TSL implementációjára hagyatkozó elektronikus aláírási alkalmazások, szolgáltatások vagy termékek esetében a következő **általános használati iránymutatások** érvényesülnek:

A „CA/QC”„Sti” bejegyzés (melyet – a minősített tanúsítványkiállítási bejegyzéshez hasonlóan – a „Sie” additionalServiceInformation (szolgáltatás további adatai) bővítménnyel „RootCA/QC”-ként (gyökértanúsítvány-kiállítási szolgáltatásnak) minősítenek)

— jelzi, hogy az „Sdi”-ben azonosított tanúsítványkiadótól (és ugyanígy az „Sdi”-ben azonosított legfelső szintű hitelesítésszolgáltatóval kezdődő szolgáltatói hierarchiából) származó, valamennyi kiállított végfelhasználói tanúsítvány minősített tanúsítvány, feltéve, hogy ez szerepel magában a tanúsítványban a megfelelő minősített tanúsítványra vonatkozó nyilatkozat (pl. a biztonságos aláírás-létrehozó eszközön alapuló minősített tanúsítványra vonatkozó nyilatkozat) és vagy az ETSI által meghatározott QCP(+) objektumazonosítók használata útján (és ezt a felügyeleti/akkreditáló szerv biztosítja, lásd fentebb az „általános szerkesztési iránymutatásokat”).

  Megjegyzés: ha nem szerepel „Sie”„Qualification” (minősítés) adat, vagy ha valamely minősített tanúsítványként feltüntetett végfelhasználói tanúsítvány nem azonosítható pontosabban valamely kapcsolódó „Sie” bejegyzés révén, a minősített tanúsítványban található „machine-processable” (géppel feldolgozható) adat helyessége tekintetében felügyelet/akkreditáció szükséges. Ez annyit jelent, hogy a megfelelő minősített tanúsítványra vonatkozó nyilatkozatok (azaz minősített tanúsítványra vonatkozó nyilatkozat, biztonságos aláírás-létrehozó eszközön alapuló minősített tanúsítványra vonatkozó nyilatkozat) és/vagy az ETSI által meghatározott QCP(+) objektumazonosítók használata vagy annak mellőzése bizonyosan megfelel annak, amit a minősített tanúsítványt kiállító hitelesítésszolgáltató állít.

▼C1

— **és HA** szerepel a „Sie”„Qualification” (minősítés) adat, a fenti alapértelmezett használatértelmezési szabályon túlmenően azokat a tanúsítványokat, amelyeket ezen „Sie”„Qualification” (minősítés) bejegyzés révén is azonosítanak – amit a tanúsítványcsoportok további azonosítására szolgáló „filters” (szűrők) sorozata elvén hoznak létre, és amely további adatokat is szolgáltat az „SSCD support” (a biztonságos aláírás-létrehozó eszközzel való támogatottság) és/vagy a „Legal person as subject” (jogi személy címzett) mezőkről (pl. a hitelesítési rend bővítményben egyedi objektumazonosítókat tartalmazó és/vagy egyedi „Key usage” (fő felhasználás) tulajdonságokkal rendelkező tanúsítványok, és/vagy egy adott tanúsítványmezőben vagy bővítményben megjelenő egyedi érték használatával szűrt tanúsítványok stb.) –, a „qualifiers” (minősítők) alábbi, a megfelelő minősített tanúsítvány adathiányát kompenzáló csoportjai szerint kell vizsgálni:

— a biztonságos aláírás-létrehozó eszközzel való támogatottság jelölésére:

  — „QCWithSSCD” minősítő érték, amelynek jelentése: „QC supported by an SSCD” (a minősített tanúsítvány biztonságos aláírás-létrehozó eszközön alapul), vagy

  — „QCNoSSCD” minősítő érték, amelynek jelentése „QC not supported by an SSCD” (a minősített tanúsítvány nem biztonságos aláírás-létrehozó eszközön alapul), vagy

  — „QCSSCDStatusAsInCert” minősítő érték, amelynek jelentése, hogy a biztonságos aláírás-létrehozó eszközzel való támogatottságra vonatkozó adat biztosan szerepel minden minősített tanúsítványban az ezen minősített tanúsítványkiállítási bejegyzés „Sdi”–„Sie” mezője alapján,

  ÉS/VAGY

— a jogi személy részére történő kiállítás jelölésére:

  — „QCForLegalPerson” minősítő érték, melynek jelentése: „Certificate issued to a Legal Person” (a tanúsítványt jogi személy részére állították ki).

2.4. *A „CA/QC” szolgáltatásokat támogató, de a „CA/QC”„Sdi”-nek részét nem képező szolgáltatások*

Olyan eseteknek is ide kell tartozniuk, amikor a tanúsítvány-visszavonási listákat és a valós idejű tanúsítvány-lekérdezésre adott válaszokat nem minősített tanúsítványt kiállító hitelesítésszolgáltatótól származó („CA/QC”) kulccsal írják alá. Ez megtehető olyan módon, hogy ezeket a szolgáltatásokat eleve ilyenként jegyzik be a megbízható szolgáltatók megbízható állapotlistán alapuló listájába (azaz egy olyan additionalServiceInformation [szolgáltatás további adatai] bővítménnyel tovább minősített „Service type identifier” [szolgáltatástípus-azonosító] azonosítóval, amely tükrözi azt, hogy a valós idejű tanúsítvány-lekérdezési vagy a tanúsítvány-visszavonási lista szolgáltatás része a minősített tanúsítvány kiállítási szolgáltatásnak, pl. „OCSP/QC”, illetve „CRL/QC” szolgáltatástípussal), mivel ezek a szolgáltatások a minősített tanúsítvány hitelesítési szolgáltatások nyújtásához kapcsolódó, felügyelt/akkreditált „qualified” (minősített) szolgáltatásnak tekinthetőek. Természetesen úgy kell tekinteni, hogy azok a valós idejű tanúsítványlekérdezés-válaszadó egységek vagy tanúsítványvisszavonásilista-kiadók, amelyek tanúsítványait a minősített tanúsítványkiállítási szolgáltatások hierarchiájába bejegyzett tanúsítványkiadók írják alá, „valid” (érvényes) státusszal rendelkeznek és megfelelnek a bejegyzett minősített tanúsítványkiállítási szolgáltatás státusértékének.

Hasonló rendelkezés vonatkozhat azokra a („CA/PKC” szolgáltatástípusú) fokozott biztonságú tanúsítványt kiállító hitelesítési szolgáltatásokra, amelyek az alapértelmezett ETSI szolgáltatástípusokat használják.

Felhívjuk a figyelmet arra, hogy a megbízható szolgáltatók listája megbízható szolgáltatások moduljának tartalmaznia KELL visszavonási szolgáltatásokat, amennyiben a vonatkozó adatok nem szerepelnek a végtanúsítványok AIA-mezőjében, illetve ha azokat nem a listán szerepelő tanúsítványkiadó írja alá.

2.5. *Az interoperábilis minősített tanúsítványprofil felé*

Főszabályként a szolgáltatásbejegyzések (különféle „Sdi”-k) számának a lehető legnagyobb mértékben történő egyszerűsítésére (csökkentésére) kell törekedni. Ezt azonban egyensúlyba kell hozni azon szolgáltatások megfelelő azonosításával, amelyek a minősített tanúsítványok kiállításához és azon megbízható információk megadásához kapcsolódnak, hogy ezek a minősített tanúsítványok biztonságos aláírás-létrehozó eszközön alapulnak-e (amennyiben ez az adat a minősített tanúsítványból hiányzik).

▼C1

Ideális esetben a „Sie” mező és a „Qualification” (minősítés) bővítmény használatát szigorúan az ilyen módon megoldandó esetekre kell korlátozni, mivel a minősített tanúsítványok elegendő adatot tartalmaznak az állított minősített státus, illetve a biztonságos aláírás-létrehozó eszközzel való támogatottság megléte vagy hiánya tekintetében.

A tagállamoknak lehetőség szerint szorgalmazniuk kell az interoperábilis minősített tanúsítványprofilok elfogadását és használatát.

3. **A megbízható szolgáltatók listája egységes sablonjának felépítése**

A tagállami megbízható szolgáltatók listájához javasolt egységes sablon a következő adatkategóriák szerint épül fel:

1. A megbízható szolgáltatók listájára és annak kiállítási rendszerére vonatkozó adatok.

2. A rendszer keretében felügyelt/akkreditált minden hitelesítésszolgáltató egyértelmű azonosítására alkalmas adatokat tartalmazó mezők sorozata (ez nem kötelező sorozat, azaz ha nem használják, a listát üresnek kell tekinteni, ami annyit jelent, hogy az adott tagállamban a megbízható szolgáltatók listájának összefüggésében egy hitelesítésszolgáltatót sem felügyelnek/akkreditáltak).

3. A listán szereplő minden egyes hitelesítésszolgáltató esetében az általa nyújtott felügyelt/akkreditált hitelesítési szolgáltatások egyértelmű azonosítására alkalmas adatokat tartalmazó mezők sorozata (ennek a sorozatnak legalább egy bejegyzést kell tartalmaznia).

4. Minden egyes felügyelt/akkreditált hitelesítési szolgáltatás esetében az adott szolgáltatás aktuális státusa és a státuselőzmények.

A minősített tanúsítványt kiállító hitelesítésszolgáltatókkal összefüggésben a listán feltüntetendő felügyelt/akkreditált hitelesítési szolgáltatások egyértelmű azonosításakor figyelembe kell vennie azokat a helyzeteket, amikor magában a minősített tanúsítványban nincs elegendő adat a „qualified” (minősített) státusról, a tanúsítvány biztonságos aláírás-létrehozó eszközzel való támogatottságáról, valamint különösen azt, hogy a (kereskedelmi) hitelesítésszolgáltatók többsége egyetlen minősített tanúsítványkiadót vesz igénybe, amely többféle – minősített és fokozott biztonságú – végfelhasználói tanúsítványt is kiállít.

Az adott elismert hitelesítésszolgáltató tekintetében a listára felvehető bejegyzések száma csökkenthető, ha egy vagy több felsőbb tanúsítványkiadási szolgáltatás létezik, pl. a tanúsítványkiadók kereskedelmi – a legfelső szintű hitelesítésszolgáltatóktól a kiállító tanúsítványkiadókig terjedő – hierarchiájával összefüggésben. Azonban még ezekben az esetekben is fenn kell tartani és biztosítani kell a minősített tanúsítványt kiállító hitelesítésszolgáltatók hitelesítési szolgáltatásai és a minősített tanúsítványnak minősülő tanúsítványcsoportok közötti egyértelmű kapcsolat elvét.

1. *A megbízható szolgáltatók listájára és annak kiállítási rendszerére vonatkozó adatok*

A következő adatok sorolandók ebbe a kategóriába:

— a megbízható szolgáltatók listájának **címkéje**, mely lehetővé teszi a megbízható szolgáltatók listájának elektronikus keresés során történő azonosítását és az olvasható formátumú lista céljának megerősítését,

— a megbízható szolgáltatók listájának **formátum- és formátumverzió-azonosítója**,

— a megbízható szolgáltatók listájának **sorozat- (vagy kiadási) száma**,

— a megbízható szolgáltatók listájának **típusára vonatkozó információ** (pl. azon tény feltüntetésére, hogy a megbízható szolgáltatók e listája az adott tagállam által az 1999/93/EK irányelvben megállapított rendelkezéseknek való megfelelés tekintetében felügyelt/akkreditált hitelesítésszolgáltatók hitelesítési szolgáltatásainak felügyeleti/akkreditációs státusáról nyújt információt),

▼C1

— a megbízható szolgáltatók listája **tulajdonosának adatai** (pl. a megbízható szolgáltatók listájának létrehozásáért, biztonságos közzétételéért és karbantartásáért felelős tagállami szerv neve, címe, elérhetősége stb.),

— azon **felügyeleti/akkreditációs rendszer(ek)re vonatkozó adatok**, amely alá a megbízható szolgáltatók listája tartozik, ideértve például a következőket:

  — annak az országnak a megjelölése, ahol a rendszert alkalmazzák,

  — a rendszerre vonatkozó adatok (rendszermodell, szabályok, feltételek, személyi hatály, típus stb.) hollétére vonatkozó információ vagy hivatkozás,

  — az (előzmény)adatok megőrzési ideje,

— a megbízható szolgáltatók listájára vonatkozó **szabályzat és/vagy jogi nyilatkozat, felelősségek, feladatok**,

— a megbízható szolgáltatók listája **kiadásának és következő tervezett frissítésének napja és időpontja**.

2. *A rendszer által elismert, minden hitelesítésszolgáltatóra vonatkozó egyértelmű azonosítást lehetővé tevő adatok*

Ez az adatkészlet legalább a következőket tartalmazza:

— a hitelesítésszolgáltató szervezet neve a hivatalos nyilvántartásba vételkor használt formában (ide tartozhat a hitelesítésszolgáltató szervezet tagállami gyakorlatnak megfelelő UID-je),

— a hitelesítésszolgáltató címe és elérhetősége,

— a hitelesítésszolgáltató további adatai, közvetlenül vagy azon hely megadásával, ahonnan ezek az adatok letölthetőek.

3. *A listán szereplő minden egyes hitelesítésszolgáltató tekintetében egy mezősorozat a hitelesítésszolgáltató által nyújtott és az 1999/93/EK irányelvvel összefüggésben felügyelt/akkreditált hitelesítési szolgáltatások egyértelmű azonosítását lehetővé tévő adatok számára*

Ez az adatkészlet a listán szereplő hitelesítésszolgáltató minden egyes hitelesítési szolgáltatása tekintetében legalább a következő adatokat tartalmazza:

— a hitelesítési szolgáltatás típusának azonosítója (pl. az azt jelző azonosító, hogy a hitelesítésszolgáltató felügyelt/akkreditált hitelesítési szolgáltatása egy minősített tanúsítványokat kiállító tanúsítványkiadó),

— a hitelesítési szolgáltatás (kereskedelmi) neve,

— a hitelesítési szolgáltatás egyértelmű azonosítását lehetővé tevő egyedi azonosító,

— a hitelesítési szolgáltatásra vonatkozó további adatok (pl. közvetlenül vagy azon hely megadásával, ahonnan ezek az adatok letölthetőek), a szolgáltatás elérhetőségére vonatkozó információk),

— minősített tanúsítványkiállítási szolgáltatás esetében egy opcionális sorozat értéksorok számára, minden értéksorban megadva a következőket:

  i. kritériumok, melyeket az „Sdi”-n belül azonosított hitelesítési szolgáltatáson belüli olyan adott szolgáltatások (pl. minősített tanúsítványok csoportja) további azonosítására (szűrésére) használnak, amelyek esetében további adatok szükségesek/állnak rendelkezésre abban a tekintetben, hogy azok biztonságos aláírás-létrehozó eszközön alapulnak-e (és/vagy azokat jogi személy részére állították-e ki); és

  ii. társított „qualifiers” (minősítők), melyek megadják, hogy a pontosabban meghatározott szolgáltatásból származó minősített tanúsítványok biztonságos aláírás-létrehozó eszközön alapulnak-e vagy sem, és/vagy az arra vonatkozó adatokat, hogy az ilyen minősített tanúsítványokat jogi személy részére állították-e ki (alapértelmezésben azok természetes személy részére kiállítottnak minősülnek).

▼C1

4. *A listára felvett minden egyes hitelesítési szolgáltatás esetében az adott szolgáltatás aktuális státusa és a státuselőzmények*

Ez az adatkészlet legalább a következőket tartalmazza:

— az aktuális státus azonosítója,

— az aktuális státus kezdetének napja és időpontja,

— a státusra vonatkozó előzményadatok.

4. **Fogalommeghatározások és rövidítések**

Ebben a dokumentumban a következő fogalommeghatározásokat és betűszavakat használjuk:

Kifejezés	Betűszó	Fogalommeghatározás
Hitelesítésszolgáltató	CSP	Az 1999/93/EK irányelv 2. cikkének (11) bekezdésében szereplő fogalommeghatározás szerint.
Tanúsítványkiadó	CA	A tanúsítványkiadó olyan hitelesítésszolgáltató, amely végfelhasználói tanúsítványok kiállításának céljaira több technikai, társított tanúsítvánnyal rendelkező titkos tanúsítványkiállítói aláírókulcsot is használhat. A tanúsítványkiadó olyan hatóság, melyet egy vagy több felhasználó tanúsítványok aláírásával és kiosztásával bíz meg. Arra is van lehetőség, hogy a tanúsítványkiadó felhasználói kulcsokat hozzon létre [ETSI TS 102 042]. A tanúsítványkiadót a tanúsítványkiállító titkos aláírókulcsához társított nyilvános kulcs tanúsításához kapcsolódó, a tanúsítványkiadó által felhasználói tanúsítványok kiállításához használt tanúsítványkiállítási tanúsítvány kiállítóra vonatkozó mezőjében szereplő azonosító adatok azonosítják. Egy tanúsítványkiadó több aláírókulccsal is rendelkezhet. Minden tanúsítványkiadói aláírókulcsot egyedi azonosító azonosít, a tanúsítványkiadó tanúsítványának kibocsátói kulcsazonosító (Authority Key Identifier) mezőjében.
Minősített tanúsítványokat kiállító tanúsítványkiadó	CA/QC	Az 1999/93/EK irányelv II. mellékletében megállapított követelményeknek megfelelő olyan tanúsítványkiadó, mely az említett irányelv I. mellékletében megállapított követelményeknek megfelelő minősített tanúsítványokat állít ki.
Tanúsítvány	Tanúsítvány	A 1999/93/EK irányelv 2. cikkének (9) bekezdésében szereplő fogalommeghatározás szerint.
Minősített tanúsítvány	QC	Az 1999/93/EK irányelv 2. cikkének (10) bekezdésében szereplő fogalommeghatározás szerint.
Aláíró	Aláíró	Az 1999/93/EK irányelv 2. cikkének (3) bekezdésében szereplő fogalommeghatározás szerint.
Felügyelet	Felügyelet	A kifejezést az 1999/93/EK irányelvben (3. cikk (3) bekezdés) meghatározott értelemben használjuk. Az irányelv előírja a tagállamok számára olyan megfelelő rendszer kialakítását, amely lehetővé teszi a területükön letelepedett és nyilvánosság számára minősített tanúsítványokat kiállító hitelesítésszolgáltatók felügyeletét, biztosítva az irányelvben megállapított rendelkezéseknek való megfelelés felügyeletét.
Önkéntes akkreditáció	Akkreditáció	Az 1999/93/EK irányelv 2. cikkének (13) bekezdésében szereplő fogalommeghatározás szerint.
Megbízható szolgáltatók listája	TL	Az adott tagállam által az 1999/93/EK irányelv vonatkozó rendelkezéseinek betartása tekintetében felügyelt/akkreditált hitelesítésszolgáltatók hitelesítési szolgáltatásainak felügyeleti/akkreditációs státusát feltüntető lista.

▼C1

Kifejezés	Betűszó	Fogalommeghatározás
Megbízhatósági állapotlista	TSL	A megbízhatósági állapotadatok ETSI TS 102231 szabványban meghatározott előírások szerinti bemutatására használt, aláírt lista.
Megbízható szolgáltatás		Az elektronikus ügyletekbe vetett bizalom és az ügyletek megbízhatóságának fokozását szolgáló szolgáltatás (mely rendszerint, de nem szükségszerűen titkosítási technikákat használ vagy bizalmas anyagokra vonatkozik) (ETSI TS 102231 szabvány).
Megbízható szolgáltató	TSP	Egy vagy több (elektronikus) megbízható szolgáltatást üzemeltető szervezet (A kifejezés a hitelesítésszolgáltatónál tágabb értelemben használatos).
Megbízható szolgáltatástoken	TrST	A megbízható szolgáltatások igénybe vételének eredményeként generált vagy kiállított fizikai vagy bináris (logikai) objektumok. A bináris megbízható szolgáltatástokenre példák a tanúsítványok, tanúsítvány-visszavonási listák, időbélyegzők és a valós idejű tanúsítvány-lekérdezésre adott válaszok.
Minősített elektronikus aláírás	QES	Minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírás, melyet az 1999/93/EK irányelv 2. cikkében meghatározott biztonságos aláírás-létrehozó eszközzel hoztak létre.
Fokozott biztonságú elektronikus aláírás	AdES	Az 1999/93/EK irányelv 2. cikkének (2) bekezdésében szereplő fogalommeghatározás szerint.
Minősített tanúsítvánnyal kísért fokozott biztonságú elektronikus aláírás	$AdES_{QC}$	Olyan elektronikus aláírás, mely megfelel a fokozott biztonságú elektronikus aláírások követelményeinek, és amelyet az 1999/93/EK irányelv 2. cikkében meghatározott minősített tanúsítvány kísér.
Biztonságos aláírás-létrehozó eszköz	SSCD	Az 1999/93/EK irányelv 2. cikkének (6) bekezdésében szereplő fogalommeghatározás szerint.

I. FEJEZET

RÉSZLETES LEÍRÁS A „FELÜGYELT/AKKREDITÁLT MEGBÍZHATÓ HITELESÍTÉSSZOLGÁLTATÓK LISTÁJÁNAK” EGYSÉGES SABLONJÁHOZ

A dokumentum következő részében a KÖTELEZŐ, a TILOS, a SZÜKSÉGES, a KELL, a TILOS/TILTOTT, a JAVASOLT, a NEM JAVASOLT, az AJÁNLOTT, a LEHET és az OPCIONÁLIS értelmezésére az RFC 2119-ben ([1]) leírtak irányadók.

►**M1** Ez a leírás az ETSI TS 102 231 v.3.1.2 szabványban szereplő leíráson és követelményeken alapul. Ha ez a leírás külön követelményt nem tartalmaz, teljes mértékben az ETSI TS 102 231 v.3.1.2 szabványnak KELL érvényesülnie. ◄ Ha a leírásban külön követelmények szerepelnek, azoknak az ETSI TS 102231 szabványban meghatározott formátumkövetelmények teljesítésekor az említett szabvány megfelelő követelményeihez képest elsőbbséget KELL élvezniük. A leírás és az ETSI TS 102231 szabvány leírása közötti ütközés esetén ennek a leírásnak KELL irányadónak lennie.

([1]) IETF RFC 2119: „Key words for use in RFCs to indicate Requirements Levels”.

▼C1

Nyelvi támogatásnak legalább angol (EN) és esetlegesen egy vagy több nemzeti nyelven KELL megvalósulnia.

A dátumok és időpontok jelölésének meg KELL felelnie az ETSI TS 102231 szabvány 5.1.4. pontjának.

Az URI-k (Uniform Resource Identifiers – egységes forrásazonosítók) használatának meg KELL felelnie az ETSI TS 102231 szabvány 5.1.5. pontjának.

A megbízható szolgáltatók listája kiállítási rendszerének adatai

Tag

TSL tag (5.2.1 pont)

Ez a mező SZÜKSÉGES, és meg KELL felelnie az ETSI TS 102231 szabvány 5.2.1 pontjának.

▼M1

———————

▼C1

Scheme Information

TSL version identifier (5.3.1. pont)

Ez a mező SZÜKSÉGES, és értéke „3” (egész szám) KELL, hogy legyen.

TSL sequence number (5.3.2. pont)

▼M1

Ez a mező SZÜKSÉGES. A TSL sorszámát KELL megadnia. A TSL első kiadásakor „1”-től indul, és ennek az egész számú értéknek a TSL újabb kiadásakor minden alkalommal nőnie KELL. A fenti „TSL version identifier” emelkedése esetén TILOS „1” értéknél újrakezdődnie.

▼C1

TSL type (5.3.3. pont)

▼M1

Ez a mező SZÜKSÉGES, és a TSL típusát adja meg. Beállítási értéke a következő KELL, hogy legyen: http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLtype/generic (Generic).

▼C1

Megjegyzés: Az ETSI TS 102231 szabvány 5.3.3. pontjának való megfelelés érdekében, valamint a megbízható szolgáltatók tagállami listája TSL implementációjának létrehozására vonatkozó ezen leírás létezésére való utaláskor ([1]), valamint a szintaktikai elemzők számára annak meghatározása lehetővé tételéhez, hogy a következő mezők ([2]) mely formája várható – amennyiben e mezők sajátos (vagy más) jelentéssel bírnak a képviselt TSL típusától (ez esetben a megbízható szolgáltatók tagállami listája) függően –, a fenti egyedi URI bejegyzése és leírása a következő KELL, hogy legyen:

([1]) Azaz az „adott tagállam által az 1999/93/EK irányelv vonatkozó rendelkezéseinek betartása tekintetében felügyelt/akkreditált hitelesítésszolgáltatók hitelesítési szolgáltatásainak felügyeleti/akkreditációs státusát feltüntető lista” (röviden: „a megbízható szolgáltatók listája”).

([2]) Ez alatt az ETSI TS 102 231- Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information szabványban megjelölt és az ebben a leírásban leírt, a megbízható szolgáltatók tagállami létrehozásának létrehozását meghatározó mezőket értjük.

▼M1

URI: (Generic): http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic

▼C1

Leírás:: A megbízható szolgáltatók tagállami listája TSL implementációját birtokló adott tagállam által az 1999/93/EK irányelvben megállapított vonatkozó rendelkezéseknek való megfelelés tekintetében közvetlen (önkéntes vagy szabályozói) felügyelet révén felügyelt/akkreditált hitelesítésszolgáltatók hitelesítési szolgáltatásai felügyeleti/akkreditációs státus listájának TSL implementációja.

Scheme operator name (5.3.4. pont)

Ez a mező SZÜKSÉGES. A megbízható szolgáltatók nemzeti listájának létrehozásáért, közzétételéért és vezetéséért felelős szervezet nevét KELL, hogy megadja. Meg KELL adnia azt a hivatalos nevet, mely alatt az e szervezethez társított szervezet vagy megbízott szervezet (pl. kormányzati közigazgatási ügynökségek) működik. Ez a hivatalos nyilvántartásba vételkor vagy felhatalmazáskor használt név KÖTELEZŐ, és erre kell címezni valamennyi hivatalos közleményt. A név többnyelvű karakterláncok sorozata KELL, hogy legyen és kötelező nyelvként angol (EN) nyelven és esetlegesen egy vagy több nemzeti nyelven KELL, hogy bevezetésre kerüljön.

Megjegyzés: valamely országnak bármely kapcsolódó operatív tevékenység vonatkozásában elkülönült felügyeleti és akkreditációs szervei is LEHETNEK. ►M1 Az egyes tagállamok feladata a Scheme operator kijelölése a megbízható szolgáltatók tagállami listájának TSL implementációja számára. ◄ Elvárás, hogy a felügyeleti szervnek, az akkreditáló szervnek és a rendszerüzemeltetőnek is saját feladat- és felelősségi köre legyen (amennyiben ezek külön szervek).

Minden olyan helyzetet, amelyben a felügyeleti, akkreditációs vagy üzemeltetési vonatkozásokért több szerv felel, egységesen ilyenként KELL megjelölni, a rendszeradatok között a megbízható szolgáltatók listájának részeként, ideértve a „Scheme information URI” (a rendszer adatainak URI-ja) (5.3.7. pont) mezőben megjelölt rendszerspecifikus adatok között ekként történő megjelölést is.

▼M1

A megnevezett Scheme operator (5.3.4. pont) a TSL-t aláíró szervezet.

▼C1

Scheme operator address (5.3.5. pont)

Ez a mező SZÜKSÉGES. A „Scheme operator name” (rendszerüzemeltető neve) mezőben (5.3.4. pont) postai és elektronikus kommunikáció céljából megjelölt jogi személy vagy megbízott szervezet címét KELL megadnia. Ennek része KELL, hogy legyen mind az 5.3.5.1. pontnak megfelelő „PostalAddress” (azaz utcanév, ország [állam vagy tartomány], [postai irányítószám], mind az ISO 3166-1 alpha-2 országkód) mező, valamint az 5.3.5.2. pontnak megfelelő „ElectronicAddress” (azaz e-mail és/vagy webhely URI) mező.

Scheme name (5.3.6. pont)

Ez a mező SZÜKSÉGES, és azt a nevet adja meg, amely alatt a rendszer üzemel. A név többnyelvű karakterláncok sorozata KELL, hogy legyen (kötelező nyelvként angol (EN) nyelven és esetlegesen egy vagy több nemzeti nyelven), a következő meghatározásnak megfelelően:

▼C1

— Az angol (EN) nyelvi változat az alábbiak szerint felépülő karakterlánc:

CC:EN_name_value

ahol:

— „CC” = a „Scheme territory” mezőben (5.3.10. használt) ISO 3166-1 alpha-2 országkód,

— „:” = elválasztó karakter,

▼M1

„EN_name_value” = Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC and its implementation in the referenced Member State’s laws.

▼C1

— Minden tagállami nemzeti nyelvi változatban a következők szerint felépülő karakterlánc KELL, hogy szerepeljen:

CC:name_value

ahol:

— „CC” = a „Scheme territory” mezőben (5.3.10. használt) ISO 3166-1 alpha-2 országkód,

— „:” = elválasztó karakter,

— „name_value” = a fenti „EN_name_value” mező nemzeti nyelvre történő hivatalos fordítása.

A rendszernévnek a névvel egyedileg kell azonosítania a „Scheme information URI” (a rendszer adatainak URI-ja) mezőben említett rendszert és biztosítania kell azt is, hogy amennyiben a rendszerüzemeltető több rendszert üzemeltet, mindegyik rendszernek megkülönböztethető nevet adjon.

A tagállamoknak és rendszerüzemeltetőknek biztosítaniuk KELL, hogy amennyiben a tagállam vagy rendszerüzemeltető több rendszert üzemeltet, mindegyik rendszernek megkülönböztethető neve legyen.

Scheme information URI (5.3.7. pont)

Ez a mező SZÜKSÉGES, és azt az egy vagy több URI-t KELL, hogy megadja, amely(ek)en a felhasználók) (a listát használók) a rendszerspecifikus adatokat megtalálhatják (kötelező nyelvként angol (EN) nyelven és esetlegesen egy vagy több nemzeti nyelven). Az URI többnyelvű mutatók sorozata KELL, hogy legyen (kötelező nyelvként angol (EN) nyelven és esetlegesen egy vagy több nemzeti nyelven). A megadott URI(k)-nak KÖTELEZŐ megadniuk az elérési utat az „appropriate information about the scheme” (megfelelő rendszeradatok) mezőhöz.

A „appropriate information about the scheme” (megfelelő rendszeradatok) mező legalább a következőket KELL, hogy tartalmazza:

— Általános bevezető adatok – melyek valamennyi tagállam esetében közösek – a megbízható szolgáltatók listájának alkalmazási köre és kontextusa, valamint az érvényesülő felügyeleti/akkreditációs rendszer tekintetében. A használandó közös szöveg a következő:

▼C1

„The present list is the TSL implementation of [*name of the relevant Member State*] »Trusted List of supervised/accredited Certification Service Providers« providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The Trusted List aims at:

— listing and providing reliable information on the supervision/accreditation status of certification services from Certification Service Providers, who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions laid down in Directive 1999/93/EC;

— facilitating the validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3.2 and Art. 7.1(a)), including information on the QC supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

The CSPs issuing Qualified Certificates (QCs) listed here are supervised by [*name of the relevant Member State*] and may also be accredited for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). The applicable »supervision« system (respectively »voluntary accreditation« system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3.3, Art. 8.1, Art. 11 (respectively, Art.2.13, Art. 3.2, Art 7.1(a), Art. 8.1, Art. 11)

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) are included in the Trusted List and the present TSL implementation at a national level on a voluntary basis.”

— Az érvényesülő felügyeleti/akkreditációs rendszer(ek)re vonatkozó külön adatok, különösen a következők ([1]):

— A minősített tanúsítványt kiállító hitelesítésszolgáltatókra vonatkozó felügyeleti rendszer adatai,

([1]) Az utolsó két adatkészlet kulcsfontosságú a listát használók számára a felügyeleti/akkreditációs rendszerek minőségének és biztonsági szintjének értékeléséhez Ezeket az adatkészleteket a megbízható szolgáltatók listája szintjén kell megadni, a „Scheme information URI” (5.3.7. pont, tagállamok által megadott információk), a „Scheme type/community/rules” (rendszertípus/közösség/szabályok) (5.3.9. pont – valamennyi tagállam esetében azonos szöveggel, és a tagállam által megadott, nem kötelező adatok révén) és a „TSL policy/legal notice” (megbízható állapotlista szabályzat/jogi figyelmeztetés) (5.3.11. pont – valamennyi tagállam esetében azonos, az 1999/93/EK irányelvre utaló szöveg, azzal, hogy minden tagállam feltüntetheti a tagállamra jellemző egyedi szöveget/hivatkozásokat) mezők használatával. A minősített tanúsítvány kiállításával nem foglalkozó hitelesítésszolgáltatók nemzeti felügyeleti/akkreditációs rendszerének szintjén meghatározott további adatokat szükség esetén (pl. több minőségi/biztonsági szint megkülönböztetése érdekében) szolgáltatási szinten lehet megadni a „Scheme service definition URI” (a rendszer szolgáltatásai meghatározásának URI-ja) (5.5.6. pont) mező használatával.

▼C1

— Adott esetben a minősített tanúsítványt kiállító hitelesítésszolgáltatókra vonatkozó nemzeti „önkéntes akkreditációs” rendszer adatai,

— Adott esetben a minősített tanúsítvány kiállításával nem foglalkozó hitelesítésszolgáltatókra vonatkozó felügyeleti rendszer adatai,

— Adott esetben a minősített tanúsítvány kiállításával nem foglalkozó hitelesítésszolgáltatók nemzeti önkéntes akkreditációs rendszerének adatai,

— Ezeknek a külön adatoknak a fentiekben felsorolt minden rendszer tekintetében tartalmazniuk KELL legalább a következőket:

— Általános leírás,

— A felügyeleti/akkreditáló szerv által a hitelesítésszolgáltatók felügyelete/akkreditációja során és a hitelesítésszolgáltatók által a felügyelet/akkreditáció tekintetében követett eljárás,

— A hitelesítésszolgáltatók felügyeletének/akkreditációjának szempontjai.

— Adott esetben a hitelesítési szolgáltatások nyújtásának eredményeként generált vagy kiállított egyes fizikai vagy bináris (logikai) objektumokra vonatkozó egyedi „qualifications” (minősítések) – amely minősítéseket a nemzeti szinten megállapított rendelkezések és követelmények teljesítése alapján adnak meg – külön adatai, ideértve a „qualification” (minősítés) jelentését és a kapcsolódó nemzeti rendelkezéseket és követelményeket.

A rendszerre vonatkozó további tagállam-specifikus adatokat önkéntes alapon LEHET megadni. Ez a következőket KELL, hogy magában foglalja:

— a felügyelők/ellenőrök kiválasztásra használt szempontok és szabályok, valamint a hitelesítésszolgáltatók vonatkozásában általuk gyakorolt felügyelet (ellenőrzés)/akkreditáció meghatározása,

— A rendszer üzemeltetésére vonatkozó egyéb kapcsolattartási és általános adatok.

Status determination approach (5.3.8. pont)

Ez a mező SZÜKSÉGES, és a státusmeghatározási megközelítés azonosítóját KELL megadnia. A következő egyedi URI-t KELL használni, a következő bejegyzésnek és leírásnak megfelelően:

URI: http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/StatusDetn/-appropriate

Leírás:: A listán szereplő szolgáltatások státusát a rendszerüzemeltető vagy képviselője határozza meg a tagállam olyan megfelelő rendszere alapján, mely lehetővé teszi a tagállam területén (vagy önkéntes akkreditáció esetében harmadik országban) letelepedett és a nyilvánosságnak az 1999/93/EK irányelv 3. cikkének (3) bekezdése (illetve 3. cikkének (2) bekezdése vagy 7. cikke (1) bekezdésének a) pontja) szerint minősített tanúsítványokat kiállító hitelesítésszolgáltatók felügyeletét (és adott esetben akkreditációját), és amely adott esetben lehetővé teszi a minősített tanúsítványok kiállításával nem foglalkozó hitelesítésszolgáltatók felügyeletét/önkéntes akkreditációját, a minősített tanúsítványok kiállításával nem foglalkozó hitelesítésszolgáltatók szolgáltatásainak az 1999/93/EK irányelvben meghatározott és az e szolgáltatások nyújtására vonatkozó nemzeti rendelkezésekben esetlegesen kiterjesztett rendelkezéseknek való megfelelés felügyeletére nemzeti szinten meghatározott, létrehozott és bevezetett, „recognised approval scheme(s)” (elismert jóváhagyási rendszer(ek) szerint.

▼C1

Scheme type/community/rules (5.3.9. pont)

Ez a mező SZÜKSÉGES, és legalább a következő bejegyzett URI-ket KELL, hogy tartalmazza:

— A megbízható szolgáltatók valamennyi tagállami listája vonatkozásában közös URI, mely az összes listára vonatkozó leíró szövegre mutat:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/common

— Ez jelzi a tagállam („TSL type”– TSL típusa) (5.3.3. pont) és „Scheme name” (5.3.6. pont) mezővel azonosított) rendszerének a rendszerek rendszerében való részvételét (azaz a TSL formájában megbízható szolgáltatók listáját közzétevő és vezető minden tagállamra mutató TSL listahivatkozás),

— A felhasználók hol szerezhetik be azokat a szabályzatokat/szabályokat, amelyek szerint a listán szereplő szolgáltatásokat értékelni KELL, és amelyek alapján a TSL típusa (lásd az 5.3.3. pontot) meghatározható,

— A felhasználók hol szerezhetik be az arra vonatkozó leírást, hogy miként kell használni és értelmezni a megbízható szolgáltatók listája TSL implementációjának tartalmát. Ezek a használati szabályok a megbízható szolgáltatók valamennyi tagállami listája esetében közösek KELL, hogy legyenek, a listán szereplő szolgáltatás típusától és a felügyeleti/akkreditációs rendszer(ek)től függetlenül.

Leíró szöveg:

„Participation in a scheme

Each Member State must create a »Trusted List of supervised/accredited Certification Service Providers« providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by the relevant Member State for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The present TSL implementation of such Trusted Lists is also to be referred to in the list of links (pointers) towards each Member State’s TSL implementation of their Trusted List, compiled by the European Commission.

Policy/rules for the assessment of the listed services

The Trusted List of a Member State must provide a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3.2 and Art. 7.1(a)), including information on the Qualified Certificate (QC) supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

▼C1

The CSPs issuing Qualified Certificates (QCs) must be supervised by the Member State in which they are established (if they are established in a Member State), and may also be accredited, for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). CSPs issuing QCs that are accredited in a Member State must still fall under the appropriate supervision system of that Member State unless they are not established in that Member State. The applicable »supervision« system (respectively »voluntary accreditation« system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3.3, Art. 8.1, Art. 11 (respectively, Art.2.13, Art. 3.2, Art 7.1(a), Art. 8.1, Art. 11)

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) may be included in the Trusted List and the present TSL implementation at a national level on a voluntary basis.

CSPs not issuing QCs but providing ancillary services, may fall under a »voluntary accreditation« system (as defined in and in compliance with Directive 1999/93/EC) and/or under a nationally defined »recognised approval scheme« implemented on a national basis for the supervision of compliance with the provisions laid down in Directive 1999/93/EC and possibly with national provisions with regard to the provision of certification services (in the sense of Art. 2.11 of the Directive). Some of the physical or binary (logical) objects generated or issued as a result of the provision of a certification service may be entitled to receive a specific »qualification« on the basis of their compliance with the provisions and requirements laid down at national level but the meaning of such a »qualification« is likely to be limited solely to the national level.

Interpretation of the TSL implementation of the Trusted List

The **general user guidelines** for electronic signature applications, services or products relying on a TSL implementation of a Trusted List according to the Annex of Commission Decision 2009/767/EK are as follows:

A »CA/QC«»Service type identifier« (»Sti«) entry (similarly a CA/QC entry further qualified as being a »RootCA/QC« through the use of »Service information extension« (»Sie«) additionalServiceInformation extension)

— indicates that from the »Service digital identifier« (»Sdi«) identified CA (similarly within the CA hierarchy starting from the »Sdi« identified RootCA) from the corresponding CSP (see associated TSP information fields), all issued end-entity certificates are Qualified Certificates (QCs) **provided** that it is claimed as such in the certificate through the use of appropriate ETSI TS 101862 defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI TS 101456 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

▼C1

Note: if no »Sie«»Qualification« information is present or if an end-entity certificate that is claimed to be a QC is not »further identified« through a related »Sie« entry, then the »machine-processable« information to be found in the QC is supervised/accredited to be accurate. That means that the usage (or not) of the appropriate ETSI defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI defined QCP(+) OIDs is ensured to be in accordance with what it is claimed by the CSP issuing QCs.

— **and IF**»Sie«»Qualification« information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this »Sie«»Qualification« entry, which is constructed on the principle of a sequence of »filters« further identifying a set of certificates, must be considered according to the associated »qualifiers« providing some additional information regarding »SSCD support« and/or »Legal person as subject« (e.g. those 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.). Those qualifiers are part of the following set of »qualifiers« used to compensate for the lack of information in the corresponding QC content, and that are used respectively:

— to indicate the nature of the SSCD support:

— »QCWithSSCD« qualifier value meaning »QC supported by an SSCD«, or

— »QCNoSSCD« qualifier value meaning »QC not supported by an SSCD«, or

— »QCSSCDStatusAsInCert« qualifier value meaning that the SSCD support information is ensured to be contained in any QC under the »Sdi«-»Sie« provided information in this CA/QC entry;

AND/OR

— to indicate issuance to Legal Person:

— »QCForLegalPerson« qualifier value meaning »Certificate issued to a Legal Person«

The general interpretation rule for any other »Sti« type entry is that the listed service named according to the »Sn« field value and uniquely identified by the »Sdi« field value has a current supervision/accreditation status according to the »Scs« 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 Technical specifications for a Common Template for the »Trusted List of supervised/accredited Certification Service Providers« in the Annex of Commission Decision 2009/767/EK for further details on the fields, description and meaning for the TSL implementation of the Member States' Trusted Lists."

▼C1

— A megbízható szolgáltatók egyes tagállami listáinak URI-ja, mely az adott tagállam listájára vonatkozó leíró szövegre KELL, hogy mutasson:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/CC,

ahol CC = a „Scheme territory” (a rendszer területi hatálya) mezőben (5.3.10. használt) ISO 3166-1 alpha-2 országkód

— Arról, hogy a felhasználók hol szerezhetik be az adott tagállam azon egyedi szabályzatait/szabályait, amelyek alapján a listán szereplő szolgáltatásokat értékelni KELL, a tagállam megfelelő felügyeleti rendszerének és önkéntes akkreditációs rendszerének megfelelően.

— Arról, hogy a felhasználók hol találják meg az adott tagállamra vonatkozó külön leírásokat arról, hogy miként kell megbízható szolgáltatók listája TSL implementációjában a nem a minősített tanúsítványok kiállításával kapcsolatos hitelesítési szolgáltatásokkal kapcsolatos tartalmát használni és értelmezni. Ez a minősített tanúsítványok kiadásával nem foglalkozó hitelesítésszolgáltatók nemzeti felügyeleti/akkreditációs rendszerek potenciális granularitásának és annak a jelzésére használható, hogy a „Scheme service definition URI” (a rendszer szolgáltatásai adatainak URI-ja)(5.5.6. pont) és a „Service information extension” (szolgáltatásadat-bővítmény) mezőket miként használják erre a célra.

A tagállamoknak további URI-ket LEHET meghatározniuk a fenti tagállamspecifikus URI-ból (azaz a specifikus URI-k hierarchiájából meghatározott URI-ket).

Scheme territory (5.3.10. pont)

E leírás alkalmazásában ez a mező SZÜKSÉGES, és a rendszer létrehozásának helye szerinti országot KELL megadnia (ISO 3166-1 alpha-2 országkód).

TSL policy/legal notice (5.3.11. pont)

E leírás alkalmazásában ez a mező SZÜKSÉGES, és a rendszer szabályzatát KELL meghatároznia, vagy a rendszer jogi státusára vagy a rendszer által a létrehozása helye szerinti országban teljesített jogszabályi követelményekre és/vagy minden olyan korlátozásra és feltételre KELL figyelmeztetnie, amely szerint a megbízható szolgáltatók listájának vezetése és közzététele történik.

Ez egy többnyelvű karakterlánc (egyszerű szöveg) KELL, hogy legyen, amely két részből áll:

— Az első rész a megbízható szolgáltatók valamennyi tagállami listája esetében közös (kötelező nyelvként angol (EN) nyelven és esetlegesen egy vagy több nemzeti nyelven), és feltünteti, hogy az irányadó jogi keretrendszer az 1999/93/EK irányelv, illetve annak végrehajtását a „Scheme Territory” (a rendszer területi hatálya) mezőben feltüntetett ország jogában szolgáló jogszabályok.

A közös szöveg angol nyelvi változata:

The applicable legal framework for the present TSL implementation of the Trusted List of supervised/accredited Certification Service Providers for [name of the relevant Member State] is the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and its implementation in [name of the relevant Member State] laws.

A szöveg magyar nyelven:

▼C1

A [tagállam neve] felügyelt/akkreditált hitelesítésszolgáltatóit tartalmazó, megbízható szolgáltatók listájának TSL-implementációjára irányadó jogi keretrendszer az elektronikus aláírásra vonatkozó közösségi keretfeltételekről szóló, 1999. december 13-i 1999/93/EK európai parlamenti és tanácsi irányelv és annak [tagállam neve] jogában történő végrehajtása.

— A második, a megbízható szolgáltatók egyes tagállami listáira jellemző rész (kötelező nyelvként angol (EN) nyelven és esetlegesen egy vagy több nemzeti nyelven) feltünteti az irányadó nemzeti jogszabályi keretre vonatkozó információkat (pl. különösen, ha az a minősített tanúsítvány kiállításával nem foglalkozó hitelesítésszolgáltatók nemzeti felügyeleti/akkreditációs rendszereihez kapcsolódik).

Historical information period (5.3.12. pont)

Ez a mező SZÜKSÉGES, és (egész számmal) azt az időtartamot KELL megadnia, amelyre a TSL előzményadatokat ad. Az egész számú érték a napok számát jelöli, és e leírás alkalmazásában legalább 3 653 KELL, hogy legyen (ami annyit jelent hogy a megbízható szolgáltatók tagállami listája TSL implementációjának KÖTELEZŐ legalább tíz évre vonatkozóan előzményadatokat tartalmaznia). Az ennél nagyobb értékeknek figyelembe kell venniük a „Scheme Territory” (a rendszer területi hatálya) (5.3.10. pont) mezőben feltüntetett országban az adatmegőrzésre vonatkozó jogszabályokat.

Pointers to other TSLs (5.3.13. pont)

E leírás alkalmazásában ez a mező SZÜKSÉGES, és – ha rendelkezésre áll – az Európai Bizottság által a megbízható szolgáltatók összes tagállami listája TSL implementációjáról mutató linkek gyűjteményre mutató hivatkozást KELL megadnia az ETSI TS 102231 szabványnak megfelelő formában. A TSL kiállítóját képviselő és az 5.5.3. pontban meghatározott módon formázott opcionális digitális azonosító használatára való felhatalmazáskor az ETSI TS 102231 szabvány 5.3.13. pontjának leírása érvényesül.

Megjegyzés: az Európai Bizottság által a megbízható szolgáltatók összes tagállami listájának TSL implementációjára mutató linkek gyűjteményének az ETSI TS 102231 szabványnak megfelelő implementációjáig ezt a mezőt TILOS/TILTOTT használni.

List issue date and time (5.3.14 pont)

Ez a mező SZÜKSÉGES, és (a Z-ként megadott egyezményes koordinált világidő formájában) a TSL kiadásának időpontját KELL megadnia, az ETSI TS 102231 szabvány 5.1.4. pontjában megadott dátum–időpont érték használatával.

Next update (5.3.15 pont)

Ez a mező SZÜKSÉGES, és (a Z-ként megadott egyezményes koordinált világidő formájában) a következő TSL kiadásának időpontját KELL megadnia, az ETSI TS 102231 szabvány 5.1.4. pontjában megadott dátum–időpont érték használatával. Értéke nulla, ha lezárt TSL-t jelöl.

A rendszerbe tartozó hitelesítésszolgáltató vagy szolgáltatás státusának időközi változása esetén a TSL-t KÖTELEZŐ újra kiadni az utolsó kiadott TSL lejárati időpontjáig.

E leírás alkalmazásában, a „Next update” (következő frissítés) mezőben szereplő dátum és időpont, illetve a „List issue date and time” (a lista kiadásának napja és időpontja) mezőben megadott értéknek TILOS/TILTOTT túllépnie a **hat (6)** hónapot.

▼C1

Distribution points (5.3.16 pont)

Ez a mező OPCIONÁLIS. A mező használata esetén meg KELL, hogy adja azt, hogy a megbízható szolgáltatók listája TSL implementációjának aktuális változatát és frissítéseit hol tették közzé. Több terjesztési pont megadása esetén azok mindegyikén az aktuális vagy frissített TSL azonos változatának KÖTELEZŐ megjelennie. A mező használata esetén annak formázása: nem üres, az RFC 3986 szabványnak ([1]) megfelelő sorozatok.

Scheme extensions (5.3.17 pont)

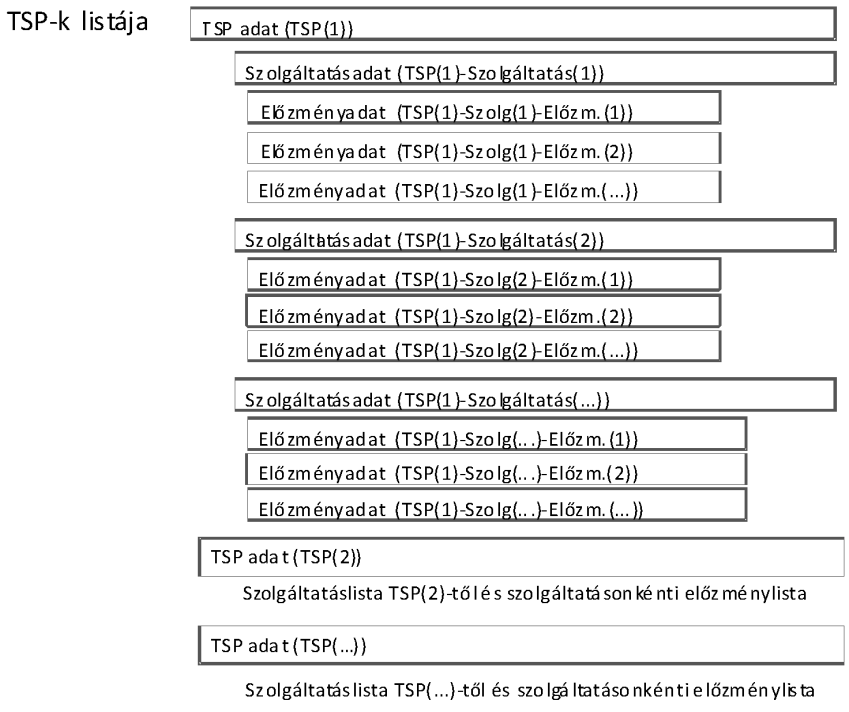
Ez a mező OPCIONÁLIS, és ebben a leírásban nem használatos.

List of Trust Service Providers

Ez a mező OPCIONÁLIS.

Amennyiben valamely tagállamban a hitelesítésszolgáltatókat a múltban vagy jelenleg nem felügyelik/akkreditálják a rendszerrel összefüggésben, ezt a mezőt el KELL hagyni. A megállapodás azonban az, hogy még ha a rendszer nem is felügyeli/akkreditálja a hitelesítésszolgáltatókat, a tagállamok a TSL-t e mező nélkül implementálják. Amennyiben a listában nem szerepel hitelesítésszolgáltató, ennek azt KELL jelentenie, hogy a „Scheme Territory” (a rendszer területi hatálya) mezőben megadott országban nincs felügyelt/akkreditált hitelesítésszolgáltató.

Amennyiben a rendszer a múltban vagy jelenleg egy vagy több hitelesítésszolgáltató szolgáltatást felügyelt/akkreditált, a mezőnek tartalmaznia KELL az ilyen felügyelt/akkreditált szolgáltatásokat nyújtó egyes hitelesítésszolgáltatókat azonosító sorozatokat, megadva az egyes hitelesítésszolgáltatók szolgáltatásainak felügyeleti/akkreditációs státusát és státuselőzményeit (az alábbi ábrában TSP = CSP).



([1]) IETF RFC 3986: „Uniform Resource Identifiers (URI): Generic syntax”.

▼C1

A TSP-k listája a fenti ábrán megadott módon szerveződik. Minden egyes TSP esetén van egy mezősorozat, mely a TSP-re vonatkozó adatokat tárolja („TSP Information”), ezt követi a szolgáltatáslista. A listán szereplő minden egyes szolgáltatás esetén van egy mezősorozat, mely a szolgáltatásadatokat („Service Information”), illetve a szolgáltatás jóváhagyási státusára vonatkozó adatokat („Service approval history”) tartalmazza.

TSP Information

TSP(1)

TSP name (5.4.1. pont)

Ez a mező SZÜKSÉGES, és a hitelesítésszolgáltatónak a rendszer keretében felügyelt vagy jóváhagyott szolgáltatásaiért felelős **jogi személy** nevét KELL megadnia. A mező többnyelvű karakterláncok sorozata (kötelező nyelvként angol (EN) nyelven és esetlegesen egy vagy több nemzeti nyelven). A névnek a hivatalos nyilvántartásba vételkor vagy felhatalmazáskor használt azon névnek KÖTELEZŐ lennie, amelyre valamennyi hivatalos közlemény szól.

TSP trade name (5.4.2. pont)

Ez a mező OPCIONÁLIS, és használata esetén meg KELL adnia a hitelesítésszolgáltató által a szolgáltatásnyújtással összefüggésben azonosításra használt másik nevet, amely a TSL-ben a szolgáltató „TSP name” (TSP neve) (5.4.1. pont) bejegyzésében szerepel.

Megjegyzés: Amennyiben egy hitelesítésszolgáltató jogi személy különböző kereskedelmi nevek alatt vagy különféle környezetekben nyújt szolgáltatást, a hitelesítésszolgáltatói bejegyzések száma megegyezhet az ilyen környezetek számával (pl. név/kereskedelmi név bejegyzések). Ehelyett az a megoldás is alkalmazható, hogy minden egyes hitelesítésszolgáltatót (jogi személyt) egyszer visznek fel a listára, és megadják a szolgáltatási környezetre vonatkozó egyedi adatokat. A tagállami rendszerüzemeltető feladata, hogy a hitelesítésszolgáltatóval megvitassa a legmegfelelőbb megközelítést, és arról megegyezzen vele.

TSP address (5.4.3. pont)

Ez a mező SZÜKSÉGES, és a „TSP name” (TSP neve) mezőben (5.4.1. pont) postai és elektronikus kommunikáció céljából megjelölt jogi személy vagy megbízott szervezet címét KELL megadnia. Ennek egyaránt része KELL, hogy legyen az 5.3.5.1. pontnak megfelelő „PostalAddress” (azaz utcanév, ország [állam vagy tartomány], [postai irányítószám] és az ISO 3166-1 alpha-2 országkód) mező, valamint az 5.3.5.2. pontnak megfelelő „ElectronicAddress” (azaz e-mail és/vagy webhely URI) mező.

TSP information URI (5.4.4. pont)

Ez a mező SZÜKSÉGES, és azokat az URI-ket KELL megadnia, amelyeken a felhasználók a hitelesítésszolgáltató egyedi adatait megtalálhatják. A mező többnyelvű hivatkozások sorozata KELL, hogy legyen (kötelező nyelvként angol (EN) nyelven és esetlegesen egy vagy több nemzeti nyelven). A hivatkozott URI(-k)-nek KÖTELEZŐ megadniuk az elérési utat a hitelesítésszolgáltató általános szerződési feltételeit, gyakorlatait, jogi kérdéseit, ügyfélszolgálati szabályzatait és a TSL CSP bejegyzésében található összes szolgáltatására vonatkozó általános jellegű információkat tartalmazó tájékoztatókhoz.

Megjegyzés: Amennyiben egyetlen hitelesítésszolgáltató jogi személy különböző kereskedelmi nevek alatt vagy különféle környezetekben nyújt szolgáltatást, és ennek nyomán minden egyes környezetre létrehoztak egy hitelesítésszolgáltatói bejegyzést, ennek a mezőnek meg KELL adnia az egyes TSP/TradeName bejegyzés alatt szereplő szolgáltatáscsoportok adatait.

▼C1

TSP information extensions (5.4.5. pont)

Ez a mező OPCIONÁLIS, és ha ez szerepel a rendszerben, a rendszerüzemeltetőnek arra LEHET használnia, hogy az ETSI TS 102231 szabvány leírásainak (5.4.5. pont) megfelelően megadja az egyedi adatokat, melyeket az adott rendszer szabályai szerint kell értelmezni.

List of Services

Ez a mező SZÜKSÉGES, és abban szerepelnie KELL a hitelesítésszolgáltató minden egyes elismert szolgáltatását azonosító sorozatnak, valamint az adott szolgáltatás jóváhagyási státusának (és az utóbbi előzményeinek). A mezőnek legalább egy szolgáltatást fel kell tüntetnie (még akkor is, ha az teljes egészében előzményadatot tartalmaz).

Mivel a listán szereplő szolgáltatások esetében e leírás szerint SZÜKSÉGES az előzményadatok megőrzése, az ilyen előzményadatokat akkor is KÖTELEZŐ megőrizni, ha a szolgáltatás jelenlegi státusa nem igényli azt, hogy a szolgáltatás a listában szerepeljen (mert pl. a szolgáltatást visszavonták). Így a hitelesítésszolgáltatót az előzmények megőrzése érdekében akkor is KÖTELEZŐ feltüntetni, ha a listán szereplő egyetlen szolgáltatása ilyen státusú.

Service Information

TSP(1) Service(1)

Service type identifier (5.5.1. pont)

▼M1

Ez a mező SZÜKSÉGES, és a szolgáltatás típusának azonosítóját KELL megadnia az aktuális TSL leírás típusa (azaz „/eSigDir-1999-93-EC-TrustedList/-TSLtype/generic”) szerint.

▼C1

Amennyiben a listán szereplő szolgáltatás minősített tanúsítványok kiállításához kötődik, a megadott URI http://uri.etsi.org/TrstSvc/Svctype/CA/QC (minősített tanúsítványokat kiállító tanúsítványkiadó) KELL, hogy legyen.

Amennyiben a listán szereplő szolgáltatás minősített tanúsítványnak nem minősülő és azok kiállítását nem támogató, megbízható szolgáltatástokenek kiadásához kapcsolódik, a megadott URI az ETSI 102231 szabvány e területre vonatkozó D.2 pontjában felsorolt URI-k egyike KELL, hogy legyen. Ennek azon megbízható szolgáltatástokenek esetében is érvényesülnie KELL, amelyekre a tagállam nemzeti jogszabályai szerinti egyes minősítések teljesítése tekintetében felügyelet/akkreditáció vonatkozik (például az úgynevezett minősített időbélyeg Németországban és Magyarországon), a megadott URI az ETSI 102231 szabvány e mezőre vonatkozó D.2. pontjában felsorolt URI-k egyike KELL, hogy legyen (pl. TSA a nemzeti szinten meghatározott minősített időbélyegek esetében). Adott esetben a megbízható szolgáltatástokenekre vonatkozó ilyen egyedi nemzeti minősítést a szolgáltatásbejegyzésnél LEHET megadni, és erre a célra az 5.5.9. pontban szereplő [„Service information extension” (szolgáltatásadat-bővítmény)] additionalServiceInformation (szolgáltatás további adatai) bővítményt KELL használni.

▼C1

Általános alapértelmezett elvként a megbízható szolgáltatók listájára felvett hitelesítésszolgáltatók esetében minden egyes X.509v3 tanúsítványhoz egy szolgáltatásbejegyzésnek KELL tartoznia (pl. a megbízható szolgáltatók listáján szereplő, minősített tanúsítványt közvetlenül kiállító hitelesítésszolgáltató – így a minősített tanúsítványokat (közvetlenül) kiállító tanúsítványkiadó – esetében). Egyes körültekintően meghatározott körülmények esetében és gondosan irányított és jóváhagyott feltételek mellett a tagállami felügyeleti szerv/akkreditáló szervnek LEHET döntenie a gyökértanúsítvány- vagy felső szintű tanúsítványkiadó (pl. a végfelhasználói tanúsítványok közvetlen kiállításával nem foglalkozó, de a hitelesítésszolgáltatók hierarchiáját a végfelhasználóknak minősített tanúsítványt kiállító tanúsítványkiadók felé hitelesítő szolgáltatók) X.509v3 tanúsítványának a listán szereplő hitelesítésszolgáltató szolgáltatásjegyzékében szereplő egyetlen bejegyzés „Sdi”-jeként történő használata mellett. A tagállamoknak körültekintően mérlegelniük kell és jóvá kell hagyniuk a gyökértanúsítvány- vagy felső szintű tanúsítványkiadó X.509v3 tanúsítványának a megbízható szolgáltatók listáján „Sdi” értékként történő használatának következményeit (előnyeit vagy hátrányait). ([1]). Emellett, az alapértelmezett elvtől való ezen engedélyezett kivétel alkalmazásakor a tagállamnak KÖTELEZŐ megadnia a hitelesítési elérési útvonal felépítését és ellenőrzését lehetővé tevő szükséges dokumentációt.

Megjegyzés: az olyan TSP-ket, mint amilyenek a minősített tanúsítványt kiállító hitelesítésszolgáltatók hitelesítési szolgáltatásainak részét képező, és azok aláírására külön-külön kulcspárt használó valós idejű tanúsítványlekérdezés-válaszadó egységek és tanúsítványvisszavonásilista-kiadók, fel LEHET tüntetni a listán ebben a TSL sablonban is, a következő URI-kombináció használatával:

— „Service type identifier” (szolgáltatástípus-azonosító) (5.5.1. pont) értéke:

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/valós idejű tanúsítvány-lekérdezés

a következő „Service information extension” (szolgáltatásadat-bővítmény) (5.5.9. pont) additionalServiceInformation (szolgáltatás további adatai) bővítmény (5.8.2.) értékkel együtt:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/OCSP-QC

Leírás: olyan tanúsítványstátusz-szolgáltató, mely a minősített tanúsítványt kiállító hitelesítésszolgáltatói szolgáltatások részeként valós idejű tanúsítvány-lekérdezési szervert üzemeltet.

— „Service type identifier” (szolgáltatástípus-azonosító) (5.5.1. pont) értéke:

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL

a következő „Service information extension” (szolgáltatásadat-bővítmény) (5.5.9. pont) additionalServiceInformation (szolgáltatás további adatai) bővítmény (5.8.2) értékkel együtt:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/CRL-QC

Leírás: olyan tanúsítványstátusz-szolgáltató, amely a minősített tanúsítványt kiállító hitelesítésszolgáltatói szolgáltatások részeként tanúsítvány-visszavonási listát vezet.

— „Service type identifier” (szolgáltatástípus-azonosító) (5.5.1. pont) értéke:

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

([1]) A gyökértenúsítvány-kiadó X.509v3 tanúsítvány listán szereplő szolgáltatás „Sdi” értékként történő használata arra fogja kényszeríteni a rendszerüzemeltetőt, hogy a gyökértenúsítvány-kiadó alatti valamennyi hitelesítési szolgáltatást egységként kezelje a „supervision/accreditation status” (felügyeleti/akkreditációs státus) tekintetében. Pl. a listán szereplő györkérhierarchiában szereplő egyetlen tanúsítványkiadó által kért státusváltoztatás az egész hierarchiát erre a státusra kényszeríti.

▼C1

a következő „Service information extension” (szolgáltatásadat-bővítmény) (5.5.9. pont) additionalServiceInformation (szolgáltatás további adatai) bővítmény (5.8.2) értékkel együtt:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/RootCA-QC

Leírás: olyan legfelső szintű hitelesítésszolgáltató, melytől kezdődően meghatározható a tanúsítási elérési útvonal egészen a minősített tanúsítványokat kiállító tanúsítványkiadóig.

— „Service type identifier” (szolgáltatástípus-azonosító) (5.5.1. pont) értéke:

http://uri.etsi.org/TrstSvc/Svctype/TSA

a következő „Service information extension” (szolgáltatásadat-bővítmény) (5.5.9. pont) additionalServiceInformation (szolgáltatás további adatai) bővítmény (5.8.2.) értékkel együtt:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/TSS-QC

Leírás: olyan időbélyegzési szolgáltatás, amely a minősített tanúsítványt kiállító hitelesítésszolgáltatói szolgáltatások részeként olyan időbélyegeket ad ki, amelyeket a minősített elektronikus aláírások érvényessége megállapításakor fel lehet használni az aláírás minősített tanúsítvány visszavonásakor vagy lejáratakor az aláírás érvényességéről való meggyőződéshez és az érvényesség kiterjesztéséhez.

Service name (5.5.2. pont)

Ez a mező SZÜKSÉGES, és azt a nevet KELL megadnia, amely alatt „TSP name” (TSP név) (5.4.1. pont) mezőben azonosított hitelesítésszolgáltató a „Service type identifier” (szolgáltatástípus-azonosító) (5.5.1. pont) mezőben azonosított szolgáltatásokat nyújtja. A mező többnyelvű karakterláncok sorozata KELL, hogy legyen (kötelező nyelvként angol (EN) nyelven és esetlegesen egy vagy több nemzeti nyelven).

Service digital identity (5.5.3. pont)

Ez a mező SZÜKSÉGES, és a „Service type identifier” (szolgáltatástípus-azonosító) (5.5.1. pont) mezőben megadott típusú szolgáltatás egyedi digitális azonosítójának legalább egy olyan formáját KELL megadnia, amellyel a szolgáltatás kétségtelenül azonosítható.

Ebben a leírásban az e mezőben használt digitális azonosító az a megfelelő X.509v3 tanúsítvány KELL, hogy legyen, amely a hitelesítésszolgáltató a „Service type identifier” (szolgáltatástípus-azonosító) (5.5.1. pont) mezőben meghatározott típusú szolgáltatások nyújtásához használt nyilvános kulcsa (pl. a gyökértanúsítvány-kiállítási szolgáltatáshoz használt kulcs, a tanúsítványok aláírásához ([1]), vagy időbélyegek kiadásához vagy a tanúsítvány-visszavonási listák aláírásához vagy a valós idejű tanúsítvány-lekérdezésekre való válaszadás aláírásához használt kulcs). Ezt a kapcsolódó X.509v3 tanúsítványt (a hitelesítésszolgáltató által a listán szereplő szolgáltatásokhoz használt nyilvános kulcs megtestesítője) KELL használni minimálisan szükséges digitális azonosítóként. További azonosítókat is LEHET használni az alábbiak szerint, de valamennyiüknek ugyanarra az azonosítóra (pl. a kapcsolódó X.509v3 tanúsítványra) KÖTELEZŐ hivatkozniuk.

([1]) Ez lehet a végfelhasználói tanúsítványokat (pl. CA/PKC, CA/QC) kiállító tanúsítványkiadó tanúsítványa **vagy** azon megbízható legfelső szintű hitelesítésszolgáltató tanúsítványa, amelynek elérési útja egészen a végfelhasználói tanúsítványokig megtalálható. Attól függően, hogy ez az adat, illetve a megbízható gyökérhierarchiában kiállított egyes végfelhasználói tanúsítványokban szereplő adatok felhasználhatóak-e a minősített tanúsítvány megfelelő tulajdonságainak egyértelmű meghatározására, előfordulhat, hogy ezt az adatot („Service digital identity” – a szolgáltatás digitális azonosítója) is meg kell adni a „Service information extensions” (szolgáltatásadat bővítmény) kitöltésével (lásd az 5.5.9 pontot).

▼C1

a) a tanúsítvány megkülönböztetésre alkalmas neve, amely a hitelesítésszolgáltató „Service type identifier” (szolgáltatástípus-azonosító) mezőben (5.5.1. pont) megadott szolgáltatása keretében történő elektronikus aláírásai érvényességének ellenőrzésére használható;

b) a kapcsolódó nyilvános kulcsazonosító (pl. X.509v3 SubjectKeyIdentifier vagy SKI érték);

c) a kapcsolódó nyilvános kulcs.

Általános alapértelmezett elvként a digitális azonosítónak (azaz a kapcsolódó X.509v3 tanúsítványnak) TILOS/TILTOTT többször is szerepelnie a megbízható szolgáltatók listájában, azaz egyetlen bejegyzésnek KELL szerepelnie a megbízható szolgáltatók listájában szereplő hitelesítésszolgáltató listában szereplő minden egyes hitelesítési szolgáltatásának X.509v3 tanúsítványa tekintetében. Viszont „Sdi” értékként egyetlen szolgáltatási bejegyzés esetében egyetlen X.509v3 tanúsítványt KELL használni.

(1) megjegyzés: az egyetlen eset, amelyben a fenti általános alapértelmezett elv esetleg nem alkalmazható, az a helyzet, amikor egyetlen X.509v3 tanúsítványt használnak olyan különböző típusú megbízható szolgáltatástokenek kiadásakor, amelyekre eltérő felügyeleti/akkreditációs rendszerek vonatkoznak, például a hitelesítésszolgáltató egyetlen X.509v3 tanúsítványt használ egyfelől a megfelelő felügyeleti rendszer alapján történő minősített tanúsítvány kiállításhoz, másfelől pedig az eltérő felügyeleti/akkreditációs státusú fokozott biztonságú tanúsítványok kiállításakor. Ebben a példában két eltérő „Sti” értékű (pl. a példában CA/QC, illetve CA/PKC), de azonos „Sdi” értékű (a kapcsolódó X.509v3 tanúsítvány) bejegyzést kell használni.

Az implementációk ASN.1 vagy XML alapúak és meg KELL felelniük az ETSI TS 102231 szabvány leírásának (az ASN.1 alapút lásd az ETSI TS 102231 szabvány A. mellékletében, az XML alapút pedig ugyanezen szabvány B. mellékletében).

(2) megjegyzés: Amennyiben az azonosított szolgáltatásbejegyzés vonatkozásában további „minősítő” adatot kell megadni, a rendszerüzemeltető adott esetben meg KELL, hogy fontolja a „Service information extension” (szolgáltatásadat-bővítmény) mezőnek (5.5.9. pont) egy additionalServiceInformation (szolgáltatás további adatai) bővítménnyel (5.8.2. pont) való kiegészítését, az ilyen további minősítő adat céljának megfelelően. Emellett a rendszerüzemeltető az 5.5.6. pont [„Scheme service definition URI” (a rendszer szolgáltatásai adatainak URI-ja)] használata mellett is dönthet.

Service current status (5.5.4. pont)

Ez a mező SZÜKSÉGES, és a szolgáltatás státusának azonosítóját KELL megadnia az alábbi URI-k egyikének használatával:

▼C2

— **Under Supervision (Felügyelt)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision),

— **Supervision of Service in Cessation (Felügyelet megszüntetés alatt)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/-supervisionincessation),

— **Supervision Ceased (Felügyelet megszűnt)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased),

— **Supervision Revoked (Felügyelet visszavonva)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked),

— **Accredited (Akkreditált)** (http://uri.etsi.org/TrstSvc/Svcstatus/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited),

— **Accreditation Ceased (Akkreditáció megszűnt)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationceased),

— **Accreditation Revoked (Akkreditáció visszavonva)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationrevoked).

▼C1

A fenti státusokat a megbízható szolgáltatók listájának e leírása alkalmazásában a következőképpen KELL értelmezni:

— ***Felügyelt:*** a „TSP name” (5.4.1. pont) mezőben azonosított hitelesítésszolgáltató által nyújtott, a „Service digital identity” (szolgáltatás digitális azonosítója) (5.5.3. pont) mezőben azonosított szolgáltatás jelenleg felügyelet alatt áll az 1999/93/EK irányelvben megállapított rendelkezéseknek való megfelelés tekintetében, a hitelesítésszolgáltató letelepedési helye szerinti, a „Scheme territory” (a rendszer területi hatálya) (5.3.10. pont) mezőben azonosított tagállamban.

▼M1

— ***A szolgáltatás felügyelete megszüntetés alatt:*** a „TSP name” (5.4.1. pont) mezőben azonosított CSP által nyújtott, a „Service digital identity” (5.5.3. pont) mezőben azonosított szolgáltatás jelenleg megszüntetés alatt áll, de felügyelete annak megszüntetéséig vagy visszavonásáig még fennáll. Amennyiben a megszüntetési szakasz biztosításának feladatát a „TSP name” mezőben azonosítottól eltérő jogi személy veszi át, az új vagy tartalék jogi személy (tartalék CSP) azonosítását a „Scheme service definition URI” pontban (5.5.6. pont) és a szolgáltatásbejegyzés „TakenOverBy” bővítményében (L.3.2. pont) KELL megadni.

▼C1

— ***Felügyelet megszűnt:*** a felügyeleti értékelés érvényessége lejárt anélkül, hogy a „Service digital identity” (szolgáltatás digitális azonosítója) (5.5.3. pont) mezőben azonosított szolgáltatást újraértékelték volna. A szolgáltatás jelenleg az aktuális státus dátumától kezdődően nem áll felügyelet alatt, mivel úgy tekintik, hogy a szolgáltatás már nem üzemel.

— ***Felügyelet visszavonva:*** a hitelesítésszolgáltató korábban felügyelet alatt állt szolgáltatása, és esetlegesen maga a hitelesítésszolgáltató sem felel már meg az 1999/93/EK irányelvben megállapított rendelkezéseknek, a hitelesítésszolgáltató letelepedési helye szerinti, a „Scheme territory” (a rendszer területi hatálya) (5.3.10. pont) mezőben azonosított tagállamban Ezért a szolgáltatás üzemeltetésének megszüntetését kellett kérni és azt a fenti ok miatt megszűntek kell tekinteni.

(1) megjegyzés: a „Supervision Revoked” státusérték lehet végleges státus, még abban az esetben is, ha a hitelesítésszolgáltató később teljesen beszünteti tevékenységét; ebben az esetben nincs szükség sem „Supervision of Service in Cessation” státusra, sem a „Supervision Ceased” státusra való áttérésre. Valójában a „Supervision Revoked” státusból való visszatérés egyetlen módja az 1999/93/EK irányelvben megállapított rendelkezéseknek való ismételt megfelelés – azon tagállam hatályos megfelelő felügyeleti rendszere szerint mely a megbízható szolgáltatók listájának tulajdonosa – és az „Under Supervision” státus ismételt elnyerése. A „Supervision of Service in Cessation” státus vagy a „Supervision Ceased” státus csak akkor következik be, amikor közvetlenül a hitelesítésszolgáltató szünteti be a felügyelt tevékenységeket, és nem pedig a felügyelet visszavonásakor.

— ***Akkreditált:*** a „Scheme territory” (a rendszer területi hatálya) (5.3.10. pont) mezőben azonosított tagállam képviseletében egy akkreditáló szerv elvégezte az akkreditációs értékelést és a „TSP name” (TSP neve) (5.4.1. pont) mezőben azonosított hitelesítésszolgáltató [1] által nyújtott, a „Service digital identity” (szolgáltatás digitális azonosítója) (5.5.3. pont) mezőben azonosított szolgáltatást az 1999/93/EK irányelvben megállapított rendelkezésekkel összhangban állónak találta.

[1] Felhívjuk a figyelmet arra, hogy az akkreditált hitelesítésszolgáltató nem feltétlenül a megbízható szolgáltatók listája TSL implementációjának „Scheme territory” mezőjében megjelölt területen telepedett le (lásd az 1999/93/EK irányelv 7. cikke (1) bekezdésének a) pontját).

▼C1

(2) megjegyzés: a „Scheme territory” (a rendszer területi hatálya) (5.3.10. pont) mezőben megadott országban letelepedett, minősített tanúsítványt kiállító hitelesítésszolgáltatóval összefüggésben történő használatkor két státust, az „Accreditation Revoked” és az „Accreditation Ceased” státust „transit status”-nak (átmeneti státusnak) KÖTELEZŐ tekinteni, és azokat TILOS „Service current status” (szolgáltatás aktuális státusa) értékként használni. Amennyiben így használják, azt a „Service approval history information” (a szolgáltatás jóváhagyási előzményadatai) vagy a „Service current status” (szolgáltatás aktuális státusa) mezőben közvetlenül az „Under supervision” státusnak KÖTELEZŐ követnie, esetlegesen az itt fent meghatározott és az 1. ábrán szemléltetett bármely más felügyeleti státus feltüntetésével. A minősített tanúsítvány kiállításával nem foglalkozó hitelesítésszolgáltatókkal összefüggésben történő használatkor – amikor csak egy társított „voluntary accreditation” (önkéntes akkreditációs) rendszer létezik felügyeleti rendszer nélkül, illetve a minősített tanúsítványt kiállító olyan hitelesítésszolgáltatókkal összefüggésben történő használatkor, amikor a hitelesítésszolgáltató nem a „Scheme territory” (a rendszer területi hatálya) (5.3.10. pont) mezőben megadott országban telepedett le (pl. harmadik országban), a „Service current status” (szolgáltatás aktuális státusa) mező értékeként az „Accreditation Revoked” és „Accreditation Ceased” státusokat LEHET használni:

— ***Akkreditáció megszűnt:*** Az akkreditációsi értékelés érvényessége lejárt anélkül, hogy a „Service digital identity” (szolgáltatás digitális azonosítója) (5.5.3. pont) mezőben azonosított szolgáltatást újraértékelték volna.

— ***Akkreditáció visszavonva:*** a „TSP name” (TSP neve) (5.4.1. pont) mezőben azonosított hitelesítésszolgáltató által nyújtott, a „Service digital identity” (szolgáltatás digitális azonosítója) (5.5.3. pont) mezőben azonosított, korábban a rendszer kritériumainak megfelelőnek talált szolgáltatás, és esetlegesen maga a hitelesítésszolgáltató sem felel már meg az 1999/93/EK irányelvben megállapított rendelkezéseknek.

(3) megjegyzés: pontosan ugyanazokat a státusértékeket kell használni a minősített tanúsítványt kiállító hitelesítésszolgáltatók és a minősített tanúsítványok kiállításával nem foglalkozó hitelesítésszolgáltatók (időbélyegző szolgáltatást nyújtó és időbélyeget kiadó hitelesítésszolgáltatók, fokozott biztonságú tanúsítványokat kiadó hitelesítésszolgáltatók, stb.) esetében. Az alkalmazandó felügyeleti/akkreditációs rendszerek közötti megkülönböztetésre a „Service Type identifier” (szolgáltatástípus-azonosító) (5.5.1. pont) mezőt kell használni.

(4) megjegyzés: adott esetben további, státushoz kapcsolódó, szolgáltatási szintű „qualification” (minősítő) adatokat lehet megadni a minősített tanúsítvány kiállításával nem foglalkozó hitelesítésszolgáltatókra vonatkozó nemzeti felügyeleti/akkreditációs rendszerek szintjén, szükség esetén (pl. több minőségi/biztonsági szint megkülönböztetése érdekében). A rendszerüzemeltető a „Service information extension” (szolgáltatásadat-bővítmény) mezőnek (5.5.9. pont) egy additionalServiceInformation (szolgáltatás további adatai) bővítménnyel (5.8.2. pont) való kiegészítését az ilyen további minősítő adat megadása céljának megfelelően KELL használnia. Emellett a rendszerüzemeltető az 5.5.6. pont [„Scheme service definition URI” (a rendszer szolgáltatásai adatainak URI-ja)] használatát is választhatja.

Current status starting date and time (5.5.5. pont)

Ez a mező SZÜKSÉGES, és azt a napot és időpontot KELL megadnia, amikor az aktuális jóváhagyási státus hatályba lépett (a dátum- és időértékek meghatározása az ETSI TS 102231 szabvány 5.1.4. pontjának megfelelően történik).

Scheme service definition URI (5.5.6. pont)

Ez a mező OPCIONÁLIS, és használata esetén többnyelvű hivatkozások sorozataként meg KELL, hogy adja azokat az URI-ket, melyeken a listát használók megtalálhatják a rendszerüzemeltető által megadott rendszerspecifikus adatokat (kötelező nyelvként angol (EN) nyelven és esetlegesen egy vagy több nemzeti nyelven).

Használatuk esetén a megadott URI-(k)nek KÖTELEZŐ megadniuk az elérési utat a rendszerben meghatározott szolgáltatást leíró adatokhoz. Adott esetben a következőket LEHET idesorolni:

a) a tartalék hitelesítésszolgáltatót azonosító URI a megszűnő felügyeletű olyan szolgáltatás esetében, amelyre tartalék hitelesítésszolgáltatót adtak meg (lásd a „Service current status” [szolgáltatás aktuális státusa] mezőt – 5.5.4. pont);

▼C1

b) az azokra a dokumentumokra mutató URI-k, amelyek a felügyelt/akkreditált megbízható szolgáltatástoken-kiadási szolgáltatás nemzeti szinten meghatározott egyedi minősítésének a „Service information extension” (szolgáltatásadat-bővítmény) (5.5.9. pont) 5.8.2. pontban meghatározott additionalServiceInformation (szolgáltatás további adatai) bővítmény használatával történő használatára vonatkozó adatokat adnak meg.

Service supply points (5.5.7. pont)

Ez a mező OPCIONÁLIS, és használata esetén meg KELL, hogy adja azokat az URI-ket, amelyeken a listát használók elérhetik a szolgáltatást, egy olyan karakterlánc-sorozat megadásával, amelynek szintaktikailag KÖTELEZŐ megfelelnie az RFC 3986 szabványnak.

TSP service definition URI (5.5.8. pont)

Ez a mező OPCIONÁLIS, és használata esetén többnyelvű hivatkozások sorozataként meg KELL, hogy adja azokat az URI-ket, melyeken a listát használók megtalálhatják a TSP által megadott rendszerspecifikus adatokat (kötelező nyelvként angol (EN) nyelven és esetlegesen egy vagy több nemzeti nyelven). A megadott URI-(k)nek KÖTELEZŐ megadniuk az elérési utat a TSP által meghatározott szolgáltatást leíró adatokhoz.

Service information extensions (5.5.9. pont)

E leírás alkalmazásában ez a mező OPCIONÁLIS, de jelen KELL lennie, ha a „Service digital identity” (szolgáltatás digitális azonosítója) (5.5.3. pont) mezőben megadott adatok a szolgáltatás által kiállított minősített tanúsítványok egyértelmű azonosítására nem elegendőek, és/vagy a kapcsolódó minősített tanúsítványokban található adatok nem teszik lehetővé azon tény géppel feldolgozható azonosítását, hogy a minősített tanúsítvány biztonságos aláírás-létrehozó eszközön alapul-e ([1]).

E leírás alkalmazásában, amennyiben használata SZÜKSÉGES – pl. minősített tanúsítványkiállítási szolgáltatások esetében – egy választható „Service information extensions” („Sie” szolgáltatásadat-bővítmény) adatmezőt KELL használni (amelynek felépítésére az ETSI TS 102231 szabvány L.3.1. mellékletében meghatározott „Qualifications” (minősítők) bővítmény irányadó) egy vagy több értéksor sorozataként, amelyben minden értéksor megadja a következőket:

— (szűrők) Olyan adatok, melyeket az „Sdi” alatt azonosított hitelesítési szolgáltatáson belüli olyan adott szolgáltatások (pl. minősített tanúsítványok csoportja) további azonosítására (szűrésére) használnak, és amelyek esetében további adatok szükségesek/állnak rendelkezésre a biztonságos aláírás-létrehozó eszközzel való támogatottság (és/vagy jogi személy címzett) megléte vagy annak hiánya tekintetében, és

— az arra vonatkozó társított adatok („qualifiers” – minősítők), hogy ez a tovább azonosított szolgáltatáscsoport biztonságos vagy más aláírás-létrehozó eszközön alapul-e (amennyiben ez az adat „QCSSCDStatusAsInCert”, ez annyit jelent, hogy a társított adat ETSI-szabványoknak megfelelő, géppel feldolgozható formában ([2]) része a minősített tanúsítványnak), és/vagy az azt a tényt jelző adat, hogy az ilyen minősített tanúsítványt jogi személynek állították-e ki (alapértelmezésben a tanúsítványok természetes személy részére kiállítottnak minősülnek),

— **QCWithSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD): ez annyit jelent, hogy a hitelesítésszolgáltató biztosítja és ellenőrzi (felügyeleti modell), vagy a tagállam (illetve annak felügyeleti szerve vagy akkreditációs szerve) ellenőrzi (akkreditációs modell) azt, hogy a szolgáltatás (QCA) keretében kiállított minden minősített tanúsítványt azonosítanak a „Service digital identity” (szolgáltatás digitális azonosítója) (5.5.3. pont) mezőben, azon minősített tanúsítványok fenti (szűrő) adatokkal történő további azonosítása céljából, melyek esetében szükség van arra az adatra, hogy azok biztonságos aláírás-létrehozó eszközön **ALAPULNAK-e** (azaz a tanúsítványban szereplő nyilvános kulcshoz társított titkos kulcsot az 1999/93/EK irányelv III. mellékletének megfelelően biztonságos aláírás-létrehozó eszközön tárolják),

([1]) Lásd e dokumentum 2.2. szakaszát.

([2]) Ez az ETSI az ETSI által meghatározott, minősített tanúsítvány megfelelőségi nyilatkozat, illetve biztonságos aláírás-létrehozó eszközön alapuló minősített tanúsítványra vonatkozó nyilatkozat [ETSI TS 101 862] vagy a QCP + ETSI által meghatározott objektumazonosító [ETSI TS 101 456].

▼C1

— **QCNoSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD): ez annyit jelent, hogy a hitelesítésszolgáltató biztosítja és ellenőrzi (felügyeleti modell), vagy a tagállam (illetve annak felügyeleti szerve vagy akkreditációs szerve) ellenőrzi (akkreditációs modell) azt, hogy a (gyökértanúsítvány-kiállítási vagy minősített tanúsítvány kiállítási) szolgáltatás keretében kiállított minden minősített tanúsítványt azonosítanak a „Service digital identity” (szolgáltatás digitális azonosítója) (5.5.3. pont) mezőben, azon minősített tanúsítványok fenti (szűrő) adatokkal történő további azonosítása céljából, melyek esetében szükség van arra az adatra, hogy azok **NEM ALAPULNAK** biztonságos aláírás-létrehozó eszközön (azaz a tanúsítványban szereplő nyilvános kulcshoz társított titkos kulcsot az 1999/93/EK irányelv III. mellékletének megfelelően **nem** biztonságos aláírás-létrehozó eszközön tárolják),

— **QCSSCDStatusAsInCert** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert): ez annyit jelent, hogy a hitelesítésszolgáltató biztosítja és ellenőrzi (felügyeleti modell), vagy a tagállam (illetve annak felügyeleti szerve vagy akkreditációs szerve) ellenőrzi (akkreditációs modell) azt, hogy a szolgáltatás (QCA) keretében kiállított és a „Service digital identity” (szolgáltatás digitális azonosítója) (5.5.3. pont) mezőben, továbbá az „Sdi”-vel azonosított hitelesítési szolgáltatás szerint a fenti (szűrő) adatokkal azonosított minden olyan minősített tanúsítvány, amelyek esetében szükség van arra az adatra, hogy azok biztonságos aláírás-létrehozó eszközön alapulnak, géppel feldolgozható formában tartalmaznia KELL azt, hogy a minősített tanúsítvány biztonságos aláírás-létrehozó eszközön alapul-e vagy sem,

— **QCForLegalPerson** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson): ez annyit jelent, hogy a hitelesítésszolgáltató biztosítja és ellenőrzi (felügyeleti modell), vagy a tagállam (illetve annak felügyeleti szerve vagy akkreditációs szerve) ellenőrzi (akkreditációs modell) azt, hogy a szolgáltatás (QCA) keretében kiállított minden minősített tanúsítványt azonosítanak a „Service digital identity” (szolgáltatás digitális azonosítója) (5.5.3. pont) mezőben, azon minősített tanúsítványok fenti (szűrő) adatokkal történő további azonosítása céljából, melyek esetében szükség van arra az adatra, hogy azokat jogi személy részére állították ki, azokat jogi személy részére **ÁLLÍTOTTÁK KI**.

Ezek a minősítők csak bővítményként használhatóak, ha a szolgáltatástípus http://uri.etsi.org/TrstSvc/Svctype/CA/QC.

Ez a mező implementációspecifikus (ASN.1 vagy XML), és annak KÖTELEZŐ megfelelnie az ETSI TS 102231 szabvány L.3.1 melléklete leírásának.

▼M1

Az XML implementáció összefüggéseiben az ilyen további információk egyedi tartalmát az ETSI TS 102 231 szabvány C. mellékletében megadott xsd fájllal kell kódolni.

▼C1

Service Approval History

Ez a mező OPCIONÁLIS, de jelenléte KÖTELEZŐ, ha a „Historical information period” (5.3.12. pont) értéke nem nulla. Így e leírás céljából a rendszernek KÖTELEZŐ megőriznie az előzményadatokat. Olyan esetekben, ha az előzményadatokat meg kívánják tartani, de a szolgáltatásnak az aktuális státus előtti előzménye nincs (azaz a rendszerüzemeltető nem tartotta meg az első rögzített státus- vagy előzményadatot), ez a mező üres KELL, hogy legyen. Egyébként a TSP szolgáltatás aktuális státusának minden egyes, az ETSI TS 102231 szabvány 5.3.12. pontjában meghatározott előzményadat-időszakban történő változása tekintetében meg KELL adni az előző jóváhagyási státus adatot, a státusváltozás napja és időpontja (azaz azon nap és időpont, amelyen a következő státusváltozás hatályba lépett) szerinti csökkenő sorrendben.

▼C1

Ez az előzményadatok következőkben meghatározott sorozata KELL, hogy legyen.

TSP(1) Service(1) History(1)

Service type identifier (5.6.1. pont)

Ez a mező SZÜKSÉGES, és a szolgáltatástípus-azonosítóját KELL megadnia, a „TSP Service Information – Service type identifier" (5.5.1. pont) mezőben használt formátumban és jelentéssel.

Service name (5.6.2. pont)

Ez a mező SZÜKSÉGES, és azt a nevet KELL megadnia, amely alatt a hitelesítésszolgáltató a „TSP Service Information – Service type identifier" (5.5.1. pont) mezőben azonosított szolgáltatásokat nyújtja. a „TSP Service Information – Service name" (5.5.2. pont) mezőben használt formátumban és jelentéssel. Ez a pont nem kívánja meg azt, hogy a név megegyezzen az 5.5.2. pontban megadott névvel. A névváltozás maga az új státust igénylő körülmények egyike is LEHET.

▼M1

Service digital identity (5.6.3. pont)

Ez a mező SZÜKSÉGES, és legalább a „TSP Service Information – Service digital identity" (5.5.3. pont) mezőben használt egyedi digitális azonosító (azaz X.509v3 tanúsítvány) egy formáját KELL megadnia, az ETSI TS 102 231 szabvány 5.5.3. pontjában megadott formátumban és jelentéssel.

Megjegyzés: A szolgáltatás „Sdi" (5.5.3.) pontjában használt X.509v3 tanúsítvány értéke esetében a megbízható szolgáltatók listájában egy „Sti:Sie/additionalServiceInformation" értékhez rendelve mindössze egyetlen szolgáltatásbejegyzés szerepelhet. A szolgáltatásbejegyzéshez kapcsolódó, a szolgáltatás jóváhagyási státusára vonatkozó adatokban felhasznált „Sdi" (5.6.3. pont) szerinti adatok és az említett szolgáltatásbejegyzésben felhasznált „Sdi" (5.5.3. pont) szerinti adatok KÖTELEZŐ, hogy ugyanarra az X.509v3 tanúsítványértékre vonatkozzanak. Amennyiben egy, a listában felsorolt szolgáltatás „Sdi"-je megváltozik (azaz pl. CA/PKC vagy CA/QC tekintetében az X.509v3 tanúsítványt megújítják vagy ahhoz új kulcsot rendelnek), vagy az említett szolgáltatáshoz új „Sdi"-t hoznak létre, a kapcsolódó „Sti", „Sn" és [„Sie"] tekintetében akár azonos értékekkel is, ez azt jelenti, hogy KÖTELEZŐ, hogy a Scheme Operator az előzőtől eltérő szolgáltatásbejegyzést hozzon létre.

▼C1

Service previous status (5.6.4. pont)

Ez a mező SZÜKSÉGES, és a szolgáltatást előző státusát KELL megadnia a „TSP Service Information – Service current status" (5.5.4. pont) mezőben használt formátumban és jelentéssel.

Previous status starting date and time (5.6.5. pont)

Ez a mező SZÜKSÉGES, és azt a napot és időpontot KELL megadnia, amikor a szóban forgó előző státus hatályba lépett a „TSP Service Information – Service current status starting date and time" (5.5.5. pont) mezőben használt formátumban és jelentéssel.

Service information extensions (5.6.6. pont)

Ez a mező OPCIONÁLIS, és a rendszerüzemeltetőknek arra LEHET használnia, hogy megadják a „TSP Service Information – Service information extensions" (5.5.9. pont) mezőben használt szolgáltatásspecifikus egyedi adatokat.

▼C1

TSP(1) Service(1) History(2)

Megegyezik a TSP(1) Service(1) History(2) (History 1 előtt) esettel

…

TSP(1) Service(2)

Megegyezik a TSP(1) Service 2 (adott esetben)

TSP(1) Service(2) History(1) esettel

…

TSP(2) Information

Megegyezik a TSP 2 (adott esetben) esettel

Megegyezik a TSP 2 Service 1 esettel

Megegyezik a TSP 2 Service 1 History 1 esettel

…

▼M1

Signed TSL

A megbízható szolgáltatók listájának e műszaki leírás és különösen ennek IV. fejezete szerint létrehozott, emberi szemmel olvasható TSL implementációját annak eredetisége és integritása biztosítása érdekében a „Scheme operator name” (5.3.4. pont) szerint JAVASOLT aláírni ([1]). Az aláírás formátuma JAVASOLT, hogy PAdES part 3 (ETSI TS 102 778-3 ([2])) legyen, azonban LEHET PAdES part 2 (ETSI TS 102 778-2 ([3])) is a megbízható szolgáltatók listájának aláírásához használt tanúsítványok közzétételével létrehozott, egyedi megbízhatósági modell összefüggésében.

A megbízható szolgáltatók listájának e műszaki leírás szerint létrehozott, géppel feldolgozható TSL implementációját annak eredetisége és integritása biztosításának érdekében a „Scheme operator name” (5.3.4. pont) szerint KELL aláírni. A megbízható szolgáltatók listája e műszaki leírás szerint létrehozott, géppel feldolgozható TSL implementációjának a formátuma XML KELL, hogy legyen, és meg KELL, hogy feleljen az ETSI TS 102 231 szabvány B. és C. mellékletében foglalt műszaki leírásoknak.

Az aláírás formátuma XAdES BES vagy EPES KELL, hogy legyen, az XML implementációk tekintetében meghatározott ETSI TS 101 903 szabvány műszaki leírásában foglaltak szerint. Az elektronikus aláírások ilyen implementációja meg KELL, hogy feleljen az ETSI TS 102 231 szabvány B. mellékletében meghatározott követelményeknek ([4]). A következő szakaszokban meghatározzuk az aláírásra vonatkozó további általános követelményeket.

▼C1

Scheme identification (5.7.2. pont)

Ez a mező SZÜKSÉGES, és a rendszerüzemeltető által adott hivatkozást KELL megadnia, amely egyedileg azonosítja az e leírásban leírt rendszert és létrehozott TSL-t, és annak KÖTELEZŐ szerepelnie az aláírás kiszámításában. Ennek karakterláncnak vagy bitláncnak kell lennie.

([1]) Amennyiben a megbízható szolgáltatók listájának emberi szemmel olvasható TSL implementációját nem látják el aláírással, annak eredetiségét és integritását KÖTELEZŐ megfelelő egyenértékű biztonsági szintű kommunikációs csatorna alkalmazásával garantálni. Erre a célra a TLS (IETF RFC 5246: „The Transport Layer Security (TLS) Protocol Version 1.2”) ajánlott, és a TLS csatorna tanúsítványának ujjlenyomatát a tagállamoknak KÖTELEZŐ protokollon kívül (out of band) a TSL-felhasználók rendelkezésére bocsátaniuk.

([2]) ETSI TS 102 778-3 – Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced – PAdES-BES and PAdES-EPES Profiles.

([3]) ETSI TS 102 778-2 – Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic – Profile based on ISO 32000-1.

([4]) A tanúsítványt aláíró rendszerüzemeltetőt kötelező az ETSI TS 101 903 szabványban meghatározott valamelyik módszer szerinti aláírással védeni, és a ds:keyInfo-nak adott esetben tartalmaznia kell a megfelelő tanúsítványláncot.

▼M1

E leírás alkalmazásában a hozzárendelt hivatkozás a „TSL type” (5.3.3. pont), a „Scheme name” (5.3.6. pont) és a rendszerüzemeltető által a TSL elektronikus aláírására használt tanúsítvány SubjectKeyIdentifier bővítménye értékét KELL, hogy tartalmazza.

▼C1

Signature algorithm identifier (5.7.3. pont)

Ez a mező SZÜKSÉGES, és azt a titkosított algoritmust KELL megadnia, melyet az aláírás létrehozásához használtak. A használt algoritmustól függően ennek a mezőnek további paramétereket is szükségessé LEHET tennie. A mezőnek KÖTELEZŐ szerepelnie az aláírás kiszámításában.

Signature value (5.7.4. pont)

Ez a mező SZÜKSÉGES, és tartalmaznia KELL a digitális aláírás aktuális értékét. Az aláírás kiszámításában KÖTELEZŐ szerepelnie a TSL valamennyi mezőjének (az aláírásérték kivételével).

TSL extensions (5.8. pont)

expiredCertsRevocationInfo bővítmény (5.8.1. pont)

Ez a bővítmény OPCIONÁLIS. Használata esetén KÖTELEZŐ megfelelnie az ETSI TS 102231 szabvány 5.8.1. pontjának.

additionalServiceInformation (szolgáltatás további adatai) bővítmény (5.8.2. pont)

Ez OPCIONÁLIS bővítmény, használata esetén KÖTELEZŐ csak szolgáltatási szinten használni, és csak az 5.5.9. („Service information extension” [szolgáltatásadat-bővítmény]) pontban meghatározott mezőben. A bővítményt a szolgáltatás további adatainak megadására használják. Egy vagy több értéksor sorozata KELL, hogy legyen, amelyben minden értéksor megadja a következőket:

a) a további adatokat azonosító URI, pl.:

— a felügyelt/akkreditált megbízható szolgáltatástoken-kiadási szolgáltatás nemzeti szinten meghatározott egyedi minősítését megadó URI, pl.

— a minősített tanúsítvány kiállításával nem foglalkozó hitelesítésszolgáltatókra vonatkozó nemzeti felügyeleti/akkreditációs rendszer egyedi biztonsági/minőségi granularitási szintje (pl. RGS */**/*** Franciaországban, nemzeti jogszabályokban meghatározott egyedi felügyeleti státus egyes minősített tanúsítványt kiállító hitelesítésszolgáltatókra Németországban), lásd a „Service current status” (szolgáltatás aktuális státusa) – 5.5.4. pont (4) megjegyzését,

— a felügyelt/akkreditált megbízható szolgáltatástoken-kiadási szolgáltatás nemzeti szinten meghatározott egyedi jogállása (pl. nemzeti szinten meghatározott „qualified TST” (minősített megbízható szolgáltatástoken), mint Németországban vagy Magyarországon),

— vagy az „Sdi” mezőben megadott X.509v3 tanúsítványban szereplő egyedi szabályzatazonosító jelentése,

— vagy a „Service type identifier” (szolgáltatástípus-azonosító) mezőben, 5.5.1. pont, megadott URI az „Sti” mezőben azonosított szolgáltatás további olyan minősítésére, hogy az a minősített tanúsítványokat (pl. valós idejű tanúsítvány-lekérdezési minősített tanúsítvány, tanúsítvány-visszavonási lista minősített tanúsítványa és legfelső szintű hitelesítésszolgáltatói minősített tanúsítvány) kiállító hitelesítésszolgáltató részszolgáltatása;

b) egy választható lánc, mely tartalmazza a serviceInformation értéket, melynek jelentését a rendszer határozza meg (pl. *, ** vagy ***);

c) minden rendszerspecifikus formátumban megadott választható további adat.

▼**M1**

Az URI visszakövetésének olyan emberi szemmel olvasható adatokat JAVASOLT eredményeznie (legalább angolul, lehetőleg pedig egy vagy több tagállami nyelven is), amelyről úgy ítélik meg, hogy megfelelő és elegendő a listát használók számára a bővítmény megértéséhez, ideértve különösen az adott URI jelentésének magyarázatát, továbbá megadva a serviceInformation mező lehetséges értékeit és az egyes értékek magyarázatát.

Qualifications Extension (L.3.1. pont)

Leírás: Ez a mező OPCIONÁLIS, de jelen KELL lennie, ha használata SZÜKSÉGES, pl. RootCA/QC szolgáltatás vagy CA/QC szolgáltatás esetén, és amennyiben

— a „Service digital identity” mezőben megadott adatok nem elegendőek a szolgáltatás által kiállított minősített tanúsítványok egyértelmű azonosítására,

— a csatolt minősített tanúsítvány adatai nem teszik lehetővé azon tény géppel feldolgozható megállapítását, hogy a minősített tanúsítvány biztonságos aláírás-létrehozó eszközön alapul-e.

Használata esetén ezt a szolgáltatásiszint-bővítményt KÖTELEZŐ csak a „Service information extension” (5.5.9. pont) szakaszban meghatározott mezőben használni, és ennek meg KELL felelnie az ETSI TS 102 231 szabvány L.3.1. mellékletében foglalt műszaki leírásoknak.

TakenOverBy Extension (L.3.2. pont)

Leírás: Ez a mező OPCIONÁLIS, de jelen KELL lennie, ha a korábban egy CSP jogi felelősségébe tartozó szolgáltatást másik TSP vesz át, és célja a szolgáltatás jogi felelősségének formális megállapítása, illetve annak lehetővé tétele, hogy az ellenőrző szoftver bizonyos jogi információkat jelenítsen meg a felhasználó számára. Az ebben a bővítményben szereplő adatoknak összhangban KELL állniuk az 5.5.6. pont kapcsolódó felhasználásával, és meg KELL felelniük az ETSI TS 102 231 szabvány L.3.2. mellékletében foglalt műszaki leírásoknak.

▼**M1**

II. FEJEZET

A tagállamok a megbízható szolgáltatók listájának a létrehozásakor figyelembe veszik a következőket:

A nyelvkódok kisbetűvel, az országkódok pedig nagybetűvel szerepelnek.

A nyelv- és országkódok az alábbi táblázatnak megfelelően szerepelnek.

Latin betűs átírás (és a megfelelő nyelvkód megadása) esetén a szöveg latin betűs átírással és az alábbi táblázatban megadott, kapcsolódó nyelvkóddal egészül ki.

Rövid megnevezés (forrásnyelv)	Rövid megnevezés (angol)	Országkód	Nyelvkód	Megjegyzések	Latin betűs átírás
Belgique/België	Belgium	BE	nl, fr, de		
България (*)	Bulgaria	BG	bg		bg-Latn
Česká republika	Czech Republic	CZ	cs		
Danmark	Denmark	DK	da		
Deutschland	Germany	DE	de		
Eesti	Estonia	EE	et		
Éire/Ireland	Ireland	IE	ga, en		
Ελλάδα (*)	Greece	EL	el	Országkód az EU ajánlása szerint	el-Latn
España	Spain	ES	es	továbbá katalán (ca), baszk (eu), galíciai (gl)	
France	France	FR	fr		
Italia	Italy	IT	it		
Κύπρος/Kıbrıs (*)	Cyprus	CY	el, tr		el-Latn
Latvija	Latvia	LV	lv		
Lietuva	Lithuania	LT	lt		
Luxembourg	Luxembourg	LU	fr, de, lb		
Magyarország	Hungary	HU	hu		
Malta	Malta	MT	mt, en		
Nederland	Netherlands	NL	nl		
Österreich	Austria	AT	de		
Polska	Poland	PL	pl		
Portugal	Portugal	PT	pt		
România	Romania	RO	ro		

▼**M1**

Rövid megnevezés (forrásnyelv)	Rövid megnevezés (angol)	Országkód	Nyelvkód	Megjegyzések	Latin betűs átírás
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	Országkód az EU ajánlása szerint	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) Latin betűs átírás: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

———————

▼C1

IV. FEJEZET

LEÍRÁS A MEGBÍZHATÓ SZOLGÁLTATÓK LISTÁJA TSL IMPLEMENTÁCIÓJÁNAK EMBERI SZEMMEL OLVASHATÓ FORMÁJÁHOZ

A megbízható szolgáltatók listája TSL implementációjának emberi szemmel olvasható formáját közzé kell tenni, és KÖTELEZŐ biztosítani ennek elektronikus hozzáférhetőségét. A leírást az ISO 32000 szabványnak megfelelő Portable Document Format (PDF) dokumentum formájában JAVASOLT elkészíteni, és annak formátumát a PDF/A (ISO 19005) profilnak megfelelően kell kialakítani.

A megbízható szolgáltatók listája TSL implementációja PDF/A-alapú olvasható formájának a következő követelményeknek JAVASOLT megfelelnie:

▼M1

— A megbízható szolgáltatók listája emberi szemmel olvasható formátumának a címét a következő elemek összefűzésével kell megalkotni:

  — a tagállam nemzeti lobogójának képe (opcionális),

  — szóköz,

  — az ország rövid megnevezése a forrásnyelve(ke)n (a II. fejezetben szereplő táblázat első oszlopában foglaltak szerint),

  — szóköz,

  — „(”,

  — az ország rövid megnevezése angolul (a II. fejezetben szereplő táblázat második oszlopában foglaltak szerint), a zárójelen belül,

  — „):” mint záró zárójel és szeparátor,

  — szóköz,

  — „Trusted List”,

  — a tagállam rendszerüzemeltetőjének a logója (opcionális).

▼C1

— A leírás felépítésének az ETSI TS 102231 szabvány 5.1.2. szakaszában leírt logikai modellt JAVASOLT tükröznie,

— Minden megadott mezőt JAVASOLT feltüntetni, és a következők megadása JAVASOLT:

  — A mező címe (pl. „Service type identifier”),

  — A mező értéke (pl. „CA/QC”),

  — Adott esetben a mező értékének jelentése (leírása), különösen az ETSI TS 102231 szabvány D mellékletében megadottak illetve ebben a leírásban megadottak szerint, regisztrált URI-k esetében (pl. „A Certification authority issuing public key certificates”),

  — Adott esetben több természetes nyelvi változat, a megbízható szolgáltatók listája TSL implementációjában előírtak szerint,

— Legalább a „Service digital identity” (szolgáltatás digitális azonosítója) mezőben szereplő digitális tanúsítványok következő mezőit és megfelelő értékeit JAVASOLT olvasható formában megjeleníteni:

  — Verzió (Version),

  — Sorszám (Serial number),

  — Aláíró algoritmus (Signature algorithm),

  — Kiállító (Issuer),

  — Érvényesség kezdete (Valid from),

  — Érvényesség vége (Valid to),

  — Tulajdonos (Subject),

▼C1

— Nyilvános kulcs (Public key),

— Hitelesítési rend (Certificate Policies),

— Tulajdonos kulcsazonosítója (Subject Key Identifier),

— A tanúsítvány-visszavonási lista terjesztési helyei (CRL Distribution Points),

— CA kulcsazonosítója (Authority Key Identifier),

— Kulcshasználat (Key Usage),

— Alapvető típusmegkötések (Basic constraints),

— Ujjlenyomat-algoritmus (Thumbprint algorithm),

— Ujjlenyomat (Thumbprint),

— Az emberi szemmel olvasható formát könnyen nyomtatható formátumban JAVASOLT elkészíteni.

— Az emberi szemmel olvasható formátumot elektronikus úton is alá LEHET írni. Aláírása esetén KÖTELEZŐ, hogy az aláíró a rendszerüzemeltető legyen, és az aláírás módja megegyezik a megbízható szolgáltatók tagállami listáinak TSL implementációjára vonatkozó aláírási specifikációval.