

A BIZOTTSÁG VÉGREHAJTÁSI HATÁROZATA**(2013. október 14.)****a 2009/767/EK határozatnak a tagállamok által felügyelt/akkreditált megbízható hitelesítésszolgáltatók listájának létrehozása, vezetése és közzététele tekintetében történő módosításáról***(az értesítés a C(2013) 6543. számú dokumentummal történt)***(EGT-vonatkozású szöveg)****(2013/662/EU)**

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló 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) 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 szóló, 2009. október 16-i 2009/767/EK bizottsági határozat ⁽²⁾ arra kötelezi a tagállamokat, hogy tegyék közzé a minősített tanúsítvánnyal kísért, fokozott biztonságú elektronikus aláírások érvényességének ellenőrzéséhez szükséges adatokat. Ezeket az adatokat a tagállamoknak egységesen, az úgynevezett „megbízható szolgáltatók listája” használatával kell közzétenniük, amely az elektronikus aláírással kapcsolatos közösségi keretfeltételekről szóló, 1999. december 13-i 1999/93/EK európai parlamenti és tanácsi irányelvvel ⁽³⁾ összhangban a nyilvánosság számára minősített tanúsítványt kiállító és a tagállamok által felügyelt/akkreditált hitelesítésszolgáltatókra vonatkozó adatokat tartalmaz.

(2) A 2009/767/EK határozat tagállami végrehajtásával kapcsolatos gyakorlati tapasztalatok azt mutatták, hogy a megbízható szolgáltatók listája által kínált előnyök maximalizálása érdekében bizonyos javításokra van szükség. Emellett az Európai Távközlési Szabványügyi Intézet (ETSI) a megbízható szolgáltatók listájára vonatkozóan új technikai leírást (TS 119 612) tett közzé, amely ugyan a határozat jelenlegi mellékletében foglalt leíráson alapul, egyúttal viszont számos ponton javításokat tartalmaz a hatályos leíráshoz képest.

(3) Ebből kifolyólag a 2009/767/EK határozatot módosítani kell, hogy az megfeleljen az ETSI 119 612 technikai leírásnak és magában foglalja a megbízható szolgáltatók listájának megvalósítását és használatát tökéletesítő és előmozdító szükséges változásokat.

(4) Annak érdekében, hogy a tagállamok végrehajthassák a szükséges technikai módosításokat a megbízható szolgáltatók jelenlegi listáit illetően, helyénvaló, hogy e határozat 2014. február 1-jétől legyen alkalmazandó.

(5) Az e határozatban előírt intézkedések összhangban vannak a szolgáltatási irányelvvel foglalkozó bizottság véleményével,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

A 2009/767/EK határozat módosítása

A 2009/767/EK határozat a következőképpen módosul:

1. A 2. cikk a következőképpen módosul:

a) Az (1), (2) és (2a) bekezdés helyébe a következő szöveg lép:

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

(2) A tagállamok a mellékletben meghatározott leírásnak megfelelően létrehozzák és közzéteszik a megbízható szolgáltatók listája géppel feldolgozható formáját. Amennyiben valamely tagállam úgy dönt, hogy a megbízható szolgáltatókat tartalmazó listáját emberi szemmel olvasható formában is közzéteszi, a megbízható szolgáltatók listája ezen formájának meg kell felelnie a mellékletben meghatározott leírás követelményeinek.

(2a) A megbízható szolgáltatók listájának eredetisége és integritása biztosítása érdekében a lista géppel feldolgozható formáját a tagállamok elektronikus aláírással látják el. Amennyiben valamely tagállam a megbízható szolgáltatók listájának emberi szemmel olvasható formáját is közzéteszi, gondoskodik arról, hogy a megbízható szolgáltatók listája ezen formája ugyanazokat az adatokat tartalmazza, mint a géppel feldolgozható forma, és azt a tagállam elektronikus aláírással látja el, amelyhez ugyanazt a tanúsítványt alkalmazza, mint a géppel olvasható formánál.”

⁽¹⁾ HL L 376., 2006.12.27., 36. o.

⁽²⁾ HL L 274., 2009.10.20., 36. o.

⁽³⁾ HL L 13., 2000.1.19., 12. o.

b) A cikk a következő (2b) bekezdéssel egészül ki:

„(2b) A tagállamok gondoskodnak arról, hogy a megbízható szolgáltatók listája géppel feldolgozható formája a közzététele helyén – a karbantartási célok kivételével – bármely időpontban folyamatosan hozzáférhető legyen.”

c) A (3) bekezdés helyébe a következő szöveg lép:

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

- a) a megbízható szolgáltatók listája géppel feldolgozható formájának létrehozásáért, vezetéséért és közzétételéért felelős szervezet vagy szervezetek neve;
- b) a megbízható szolgáltatók listája géppel feldolgozható formájának közzétételi helye;
- c) kettő vagy több rendszerüzemeltető legalább három hónapos, elcsúsztatott érvényességi időszakokkal rendelkező nyilvános kulcsú tanúsítványa, amelyek a megbízható szolgáltatók listája géppel feldolgozható formájának elektronikus aláírására felhasználható titkos kulcsokhoz tartoznak;
- d) az a)–c) pontban említett adatokkal kapcsolatos minden változás.”

d) A szöveg a következő (3a) bekezdéssel egészül ki:

„(3a) Amennyiben valamely tagállam közzéteszi a megbízható szolgáltatók listájának emberi szemmel olvasható formáját, a (3) bekezdésben említett adatokat az emberi szemmel olvasható formára vonatkozóan is be kell jelenteni.”

2. A melléklet helyébe e határozat melléklete lép.

2. cikk

Alkalmazás

Ezt a határozatot 2014. február 1-től kell alkalmazni.

3. cikk

Címzettek

Ennek a határozatnak a tagállamok a címzettjei.

Kelt Brüsszelben, 2013. október 14-én.

a Bizottság részéről

Michel BARNIER

a Bizottság tagja

MELLÉKLET

A „FELÜGYELT/AKKREDITÁLT MEGBÍZHATÓ HITELESÍTÉSSZOLGÁLTATÓK LISTÁJA” EGYSÉGES SABLONJÁNAK TECHNIKAI LEÍRÁSA**ÁLTALÁNOS KÖVETELMÉNYEK****1. Bevezetés**

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 való megfelelés tekintetében 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.

Ezen adatoknak az elsődleges célja a minősített elektronikus aláírások (QES) és a minősített tanúsítvánnyal ellátott ⁽²⁾ fokozott biztonságú elektronikus aláírások (AdES) ⁽³⁾ ⁽⁴⁾ érvényessége ellenőrzésének támogatása.

A megbízható szolgáltatók listájában szereplő kötelező információk között minimumkövetelményként a minősített tanúsítványokat ⁽⁵⁾ kiállító, az 1999/93/EK irányelv rendelkezéseiben (a 3. cikk (2) bekezdése, a 3. cikk (3) bekezdése és a 7. cikk (1) bekezdésének a) pontja) foglaltak szerint felügyelt/akkreditált hitelesítésszolgáltatókra vonatkozó adatoknak kell szerepelniük, ideértve az elektronikus aláírások alapját képező minősített tanúsítványok adatait is, ha ez nem része a minősített tanúsítványnak, és azt is, hogy az aláírás biztonságos aláírás-létrehozó eszközzel (SSCD) ⁽⁶⁾ készült-e.

A megbízható 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 hitelesítésszolgáltatók is felvehetők, amennyiben a minősített tanúsítványokat kiállító hitelesítésszolgáltatókhoz hasonló módon akkreditálják/felügyelik vagy más nemzeti jóváhagyási rendszer szerint jóváhagyják ezeket. Egyes tagállamokban a nemzeti jóváhagyási rendszerek az alkalmazandó követelmények és/vagy a felelős szervezet tekintetében különbözhetnek a minősített tanúsítványokat kiállító hitelesítésszolgáltatókra alkalmazott felügyeleti vagy önkéntes akkreditációs rendszerektől. Ezen leírásban az „akkreditált” és/vagy „felügyelt” kifejezések magukban foglalják a nemzeti jóváhagyási rendszereket is, de a nemzeti jóváhagyási rendszerekkel kapcsolatban a megbízható szolgáltatók nemzeti listájában a tagállamok további információkat fognak közölni, többek között a minősített tanúsítványokat kiállító hitelesítésszolgáltatókra alkalmazott akkreditálási/felügyeleti rendszerekhez viszonyított esetleges eltérésekre vonatkozóan is.

Az egységes sablon az ETSI TS 119 612 v.1.1.1. (a továbbiakban: ETSI TS 119 612) szabványra ⁽⁷⁾ épül, amely az ilyen listák létrehozását, közzétételét, fellelhetőségét, a listákhoz való hozzáférést, a listák hitelesítését és integritását szabályozza.

2. A megbízható szolgáltatók listája egységes sablonjának felépítése

A megbízható szolgáltatók listája tagállamok részére szóló egységes sablonja az ETSI TS 119 612 szabvány szerint épül fel, és az alábbi adatkategóriákat tartalmazza:

1. A megbízható szolgáltatók listájának címkéje, amely lehetővé teszi a megbízható szolgáltatók listájának azonosítását elektronikus keresések során.
2. A megbízható szolgáltatók listájára és annak kiállítási rendszerére vonatkozó adatok.
3. 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 listájára való felkerülés céljából egyetlen hitelesítésszolgáltatót sem felügyelnek/akkreditáltak).
4. A listán szereplő egyes hitelesítésszolgáltatókra vonatkozóan az általuk nyújtott konkrét megbízhatósági szolgáltatások részletei, mely szolgáltatások aktuális státusát a szolgáltatók listájában rögzítik, és amelyeket a hitelesítésszolgáltató által nyújtott felügyelt/akkreditált hitelesítési szolgáltatásokat egyértelműen azonosító mezők sorozataként adnak meg. (A sorozat legalább egy bejegyzést tartalmaz).

⁽¹⁾ Az 1999/93/EK irányelv 2. cikkének 11. pontjában szereplő fogalom meghatározás szerint.

⁽²⁾ Az 1999/93/EK irányelv 2. cikkének 2. pontjában szereplő fogalom meghatározás szerint.

⁽³⁾ Ennek a dokumentumnak az angol nyelvű változatában a minősített tanúsítvánnyal ellátott fokozott biztonságú elektronikus aláírást az „AdES_{QC}” rövidítéssel jelöljük.

⁽⁴⁾ Felhívjuk a figyelmet arra, hogy számos elektronikus szolgáltatás alapul egyszerű fokozott biztonságú elektronikus aláírásokon, amelyek határokon átnyúló használata is lehetővé válik, feltéve, hogy az alapul szolgáló hitelesítési szolgáltatások (pl. fokozott biztonságú tanúsítványok kiadása) szerepelnek az akkreditált/felügyelt szolgáltatások között a megbízható szolgáltatók tagállami listájának önkéntes részében.

⁽⁵⁾ Az 1999/93/EK irányelv 2. cikkének 10. pontjában szereplő fogalom meghatározás szerint.

⁽⁶⁾ Az 1999/93/EK irányelv 2. cikkének 6. pontjában szereplő fogalom meghatározás szerint.

⁽⁷⁾ ETSI TS 119 612 v.1.1.1 (2013-06) – Elektronikus aláírások és infrastruktúrák (ESI); megbízható szolgáltatók listái (Electronic Signatures and Infrastructures (ESI); Trusted Lists).

5. A listára felvett felügyelt/akkreditált hitelesítési szolgáltatások mindegyikére vonatkozóan a fenti státus előzményeire vonatkozó adatok, amennyiben alkalmazandó.

6. A megbízható szolgáltatók listája tekintetében alkalmazott aláírás.

A minősített tanúsítványt kiállító hitelesítésszolgáltatókkal összefüggésben, a megbízható szolgáltatók listájának szerkezete és különösen a szolgáltatásokra vonatkozó (a fenti 4. pont szerinti) adatelem lehetővé teszi azt, hogy a szolgáltatásokra vonatkozó információk bővítése révén kompenzálják azokat a hiányosságokat, amikor magában a minősített tanúsítványban nincs elegendő (géppel feldolgozható) adat a „minősített” (qualified) státusról, a tanúsítvány biztonságos aláírás-létrehozó eszközzel való támogatottságáról, továbbá hogy kezeljék különösen azt a tényt, hogy a (kereskedelmi) hitelesítésszolgáltatók többsége egyetlen minősített tanúsítványkiadót vesz igénybe, amely többféle – minősített és fokozott biztonságú – végfelhasználói tanúsítványt is kiállít.

A tanúsítványkiadó szolgáltatások tekintetében az adott hitelesítésszolgáltatóhoz kapcsolódó, a listán szereplő szolgáltatási bejegyzések száma csökkenthető, amennyiben a hitelesítésszolgáltató nyilvános kulcsú infrastruktúráján (PKI) belül egy vagy több felső szintű tanúsítványkiadó szolgáltatás szerepel (például a tanúsítványkiadó szolgáltatások hierarchiájában a gyökértanúsítványtól kiindulva több tanúsítványkiadó van). Ekkor ezeket a felső szintű tanúsítványkiadó szolgáltatásokat kell feltüntetni, nem pedig a végfelhasználói tanúsítványok kiadását (azaz kizárólag a hitelesítésszolgáltató gyökértanúsítványát kell feltüntetni.) Ezekben az esetekben azonban a státusra vonatkozó adat a listában szereplő szolgáltatás alatt lévő tanúsítványkiadó szolgáltatások teljes hierarchiájára vonatkozik, és fent kell tartani azt az elvet, illetve biztosítani kell annak az elvnek az érvényesülését, amelynek értelmében a minősített tanúsítványt kiállító hitelesítésszolgáltató hitelesítési szolgáltatása és a minősített tanúsítványokként azonosítandó tanúsítványok közötti egyértelmű kapcsolatot biztosítani kell.

2.1. Az egyes adatkategóriák leírása

1. Megbízható szolgáltatók listája címke

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

A következő adatok tartoznak ebbe a kategóriába:

- a megbízható szolgáltatók listájának **formátumverzió-azonosítója**,
- a megbízható szolgáltatók listájának **sorozat- (vagy kiadási) száma**,
- a megbízható szolgáltatók listájának **típusára vonatkozó információ** (például 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),
- a megbízható szolgáltatók listája **rendszer-üzemeltetőjének (tulajdonosának) adatai** (például a megbízható szolgáltatók listájának létrehozásáért, biztonságos közzétételéért és vezetéséért 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.) fellelhetőségére 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 dátuma és időpontja**,
- a megbízható szolgáltatók listája **következő tervezett frissítése**.

3. A rendszer által felügyelt/akkreditált hitelesítésszolgáltatókra vonatkozó egyértelmű azonosítást lehetővé tevő adatok

Ez az adatkategória legalább az alábbiakat tartalmazza:

- a hitelesítésszolgáltató szervezet neve a hivatalos nyilvántartásba vételkor használt formában (ideértve a hitelesítésszolgáltató szervezet tagállami gyakorlatnak megfelelő UID azonosítóját is),
- a hitelesítésszolgáltató címe és elérhetősége,
- a hitelesítésszolgáltató további adatai, közvetlenül vagy azon hely megadásával, ahonnan ezek a további adatok letölthetők.

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

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

- szolgáltatástípus-azonosító: a hitelesítési szolgáltatás típusának azonosítója (pl. az azt jelző azonosító, hogy a hitelesítésszolgáltató felügyelt/akkreditált hitelesítési szolgáltatása egy minősített tanúsítványokat kiállító tanúsítványkiadó),
- szolgáltatás (kereskedelmi) neve: a hitelesítési szolgáltatás (kereskedelmi) neve,
- a szolgáltatás digitális azonosítója: a hitelesítési szolgáltatás egyértelmű azonosítását lehetővé tevő egyedi azonosító,
- a szolgáltatás aktuális státusa: a szolgáltatás aktuális státusának azonosítója,
- az aktuális státus kezdetének napja és időpontja,
- szolgáltatásadat-bővítmény, ha alkalmazható: a szolgáltatásra vonatkozó további adatok (pl. közvetlenül vagy azon hely megadásával, ahonnan ezek az adatok letölthetők): a rendszerüzemeltető által közölt szolgáltatásmeghatározás-adatok, hozzáférési adatok a szolgáltatásra vonatkozóan, a hitelesítésszolgáltató által közölt szolgáltatásmeghatározás-adatok, valamint szolgáltatásadat-bővítmények. például a minősített tanúsítványokat kiállító tanúsítványkiadó (CA/QC) szolgáltatásai esetében értéksorok opcionális sorozata, minden értéksorban megadva a következőket:
 - kritériumok, melyeket az azonosított megbízhatósági szolgáltatáson belüli olyan adott szolgáltatások (pl. [minősített] tanúsítványok csoportja) további azonosítására (szűrésére) használnak, amelyek esetében további adatok szükségesek/állnak rendelkezésre státusukra, valamint arra vonatkozóan, hogy azok biztonságos aláírás-létrehozó eszközön alapulnak-e és/vagy azokat jogi személy részére állították-e ki, továbbá
 - társított „minősítők” (qualifiers), melyek megadják, hogy a szolgáltatás eredményeként létrejövő tanúsítványok minősített tanúsítványoknak tekinthetők-e, és/vagy az e szolgáltatásból származó minősített tanúsítványok biztonságos aláírás-létrehozó eszközön alapulnak-e vagy sem, és/vagy az arra vonatkozó információkat, hogy az ilyen minősített tanúsítványokat jogi személy részére állították-e ki (alapértelmezésben azok természetes személy részére kiállítottak tekintendők).

5. A listán szereplő minden egyes hitelesítési szolgáltatásra vonatkozóan a szolgáltatás státusának előzményeire vonatkozó információk

6. Az aláírásérték kivételével a megbízható szolgáltatók listájának összes mezőjére vonatkozóan kiszámított aláírás

3. A megbízható szolgáltatók listájában található bejegyzések szerkesztésének szabályai

3.1. A felügyelt/akkreditált hitelesítési szolgáltatások és a szolgáltatók státusára vonatkozó információk egységes listája

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 státusának listája”.

A megbízható szolgáltatók ezen listája az adott tagállam által a hitelesítési szolgáltatások felügyeleti/akkreditációs státusával és a szolgáltatókkal kapcsolatos adatok közlésére alkalmazandó egységes eszköz:

- 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 fogalom meghatározásokat 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 hitelesítésszolgáltatókra vonatkozó követelmények) követelményeit – való megfelelés tekintetében akkreditálhatók is. Egy tagállam megfelelő felügyeleti rendszerének az adott tagállamban akkreditált minősített tanúsítványt kiállító hitelesítésszolgáltatókra is ki kell terjednie, kivéve, ha ezek nem telepedtek le ebben a tagállamban.

- Az alkalmazandó „felügyeleti” (illetve „önkéntes akkreditációs”) rendszer meghatározott, és annak meg kell felelnie az 1999/93/EK irányelvben és különösen annak 3. cikke (3) bekezdésében, 8. cikke (1) bekezdésében, 11. cikkében, (13) preambulumbekkezdésében 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) preambulumbekkezdésében 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 „elismerett 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 valamilyen külön minősítésre, de az ilyen „minősítés” hatálya valószínűleg kizárólag nemzeti szintű.

A megbízható szolgáltatókról tagállamonként egy-egy listát kell létrehozni és vezetni, az adott tagállam által felügyelt/akkreditált hitelesítésszolgáltatók hitelesítési szolgáltatásai felügyeleti és/vagy akkreditációs státusának feltüntetése érdekében. A megbízható szolgáltatók listájának legalább a minősített tanúsítványokat kiállító hitelesítésszolgáltatókat tartalmaznia kell. A megbízható szolgáltatók listáján további, nemzeti szinten meghatározott jóváhagyási rendszer szerint felügyelt vagy akkreditált hitelesítési szolgáltatások státusa is szerepelhet.

3.2. Egyetlen felügyeleti/akkreditációs státus-értéksorozat

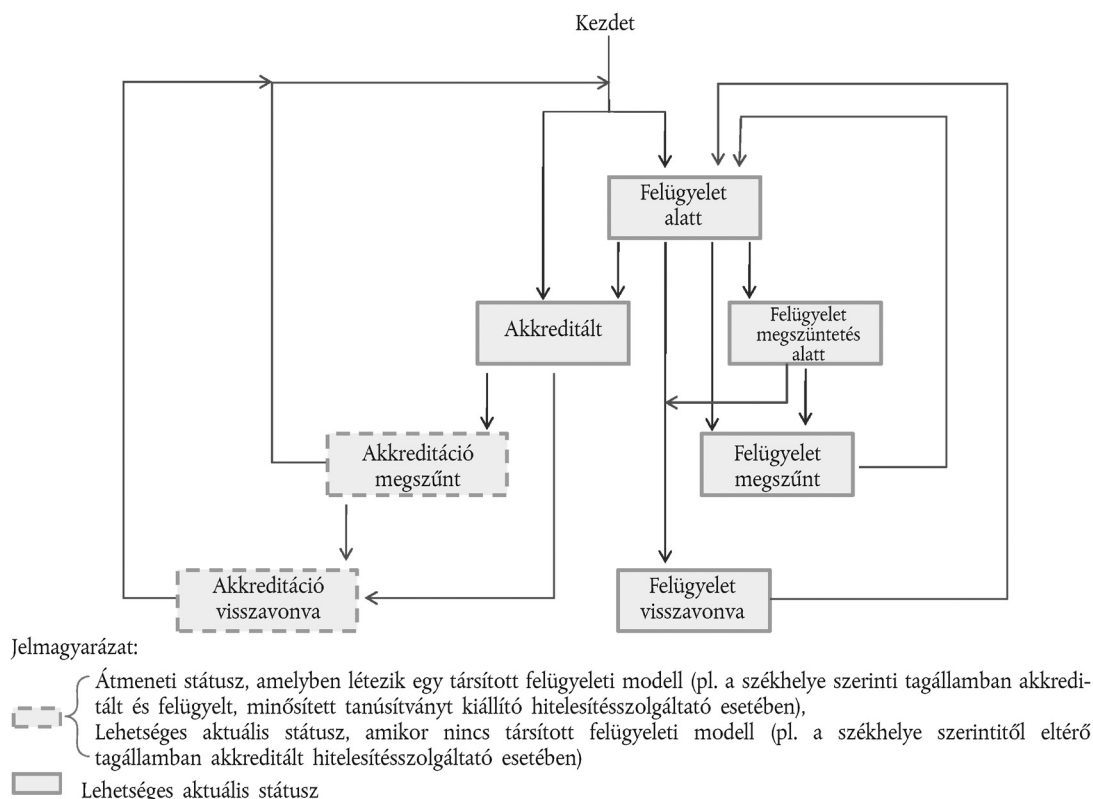
A megbízható szolgáltatók listáján azt a tényt, hogy valamely szolgáltatás „felügyelet alatt áll” vagy „akkreditált”, az aktuális státusának értéke jelzi. Továbbá a felügyeleti vagy akkreditációs státus pozitív („felügyelet alatt”, „akkreditált”, „felügyelet megszüntetés alatt”), megszűnt („felügyelet megszűnt”, „akkreditáció megszűnt”) vagy akár visszavont („felügyelet visszavonva”, „akkreditáció visszavonva”) is lehet, a megfelelő értékre állítva. 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 váltását ábrázolja:

⁽¹⁾ Például 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 önkéntes akkreditációra tér át. Megfordítva: egy másik tagállamban lévő hitelesítésszolgáltató határozhat úgy, hogy nem hagy fel az akkreditált hitelesítési szolgáltatással, hanem – például üzleti és/vagy gazdasági okokból – az akkreditációs státusról áttér a felügyeleti státusra.

1. ábra

Egy adott hitelesítési szolgáltatás felügyeleti/akkreditációs státuszának lehetséges változásai



A valamely tagállamban székhellyel rendelkező, minősített tanúsítványokat kiállító hitelesítésszolgáltató (a székhelye szerinti tagállam által biztosított) felügyelet alá tartozik és önkéntes alapon akkreditálható. Amennyiben a megbízható szolgáltatók listáján szerepel, az ilyen szolgáltatás „aktuális státusértéke” a fenti státusértékek valamelyike az aktuális státusának megfelelően, és adott esetben azt a fenti státusváltásoknak megfelelően meg kell változtatni. Azonban az „akkreditáció megszűnt” és az „akkreditáció visszavonva” státusoknak „átmeneti státusértékeknek” kell lenniük, amennyiben a minősített tanúsítványokat kiállító érintett hitelesítésszolgáltató szerepel annak a tagállamnak a megbízható szolgáltatókat tartalmazó listáján, amelyben letelepedett, mivel ezek a szolgáltatások alapértelmezés szerint felügyelet alá tartoznak (akkor is ha nincsenek vagy már nincsenek akkreditálva); amennyiben az érintett szolgáltatás a letelepedés helye szerinti tagállamtól eltérő tagállam listáján szerepel (ott van akkreditálva), ezek az értékek végleges értékek is lehetnek.

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 „elismerett jóváhagyási rendszert” hoztak vagy hoznak létre, az ilyen jóváhagyási rendszereket az alábbi két kategória egyikébe kell besorolniuk:

- „önkéntes akkreditáció” az 1999/93/EK irányelvben meghatározott szabályok szerint (2. cikk (13) bekezdése, 3. cikk (2) bekezdése, 7. cikk (1) bekezdésének a) pontja, 8. cikk (1) bekezdése, 11. cikk, (4), (11)–(13) preambulumbekkezdés),
- „felügyelet” az 1999/93/EK irányelvben előírtak szerint és nemzeti jogszabályoknak megfelelő nemzeti rendelkezések és követelmények által végrehajtva.

Ennek megfelelően a minősített tanúsítvány kiállításával nem foglalkozó hitelesítésszolgáltató állhat felügyelet alatt és lehet önkéntesen akkreditált. Amennyiben a megbízható szolgáltatók listáján szerepel, az ilyen szolgáltatás „aktuális státusértéke” a fenti státusértékek valamelyike az aktuális státusának megfelelően (lásd az 1. ábrát), és azt adott esetben a fenti státusváltásoknak megfelelően meg kell változtatni.

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 információ 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 információkat a megbízható szolgáltatók listája szintjén kell megadni, „a rendszer adatainak URI-ja” (Scheme information URI) (5.3.7. pont – a tagállamok által megadott információk), a „rendszertípus/közösség/szabályok” (Scheme type/community/rules) (5.3.9. pont – a valamennyi tagállam esetében azonos szöveggel, és a tagállam által megadott, nem kötelező adatok révén) és a „megbízhatósági állapotlista szabályzata/jogi nyilatkozat” (TSL policy/legal notice) (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 „szolgáltatásadat-bővítés” (Service information extensions) (5.5.9. pont) részét képező „további szolgáltatásadat” (additionalServiceInformation Extension) (5.5.9.4. pont) használatán keresztül. A vonatkozó technikai leírásra vonatkozó további információk az I. fejezetben található részletes leírásban találhatók.

Jóllehet a tagállamban a tagállam hitelesítési szolgáltatásainak felügyelete és akkreditációja más-más szervek feladata is lehet, elvárás, hogy egy hitelesítési szolgáltatást a listába csak egyszer vigyenek fel, és felügyeleti/akkreditációs státusát ennek megfelelően frissítsék.

3.3. 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 legkritikusabb része a lista kötelező részének kialakítása, nevezetesen „a szolgáltatások listája” (List of services) mező létrehozása a minősített tanúsítványt kiállító hitelesítésszolgáltatóként annak érdekében, hogy a lista 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 a minősített tanúsítvánnyal ellátott fokozott biztonságú elektronikus aláírás érvényességének ellenőrzéséhez (ha azt a hitelesítésszolgáltató a bejegyzésben szereplő hitelesítési szolgáltatás keretében a végfelhasználói minősített tanúsítvány tartalmával kombinálja).

A szükséges információk körébe az egyedüli legfelső szintű tanúsítványkiadó digitális szolgáltatásazonosítóján túlmenően más adatok is beletartozhatnak, így különösen az ilyen tanúsítványkiadó által kiállított tanúsítványok minősített státusát jelölő információk, továbbá az, hogy a támogatott aláírásokat biztonságos aláírás-létrehozó eszközzel hozzák-e létre. A tagállamban a megbízható szolgáltatók listájának létrehozásával, szerkesztésével és vezetésével megbízott szervezetnek 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 (QcCompliance) ⁽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 EN 319 411-2 szabványban ⁽²⁾ meghatározott QCP/QCP + hitelesítési rend objektumazonosítókat (OID). A jelenleg kiállított minősített tanúsítványok tartalmi eltérései miatt (pl. az ETSI által a minősített tanúsítványra vonatkozóan meghatározott nyilatkozatok esetleges használata) – amelynek oka a minősített tanúsítványt kiállító hitelesítésszolgáltatók részéről különböző szabványok hivatkozásként való használata, e szabványok egyedi értelmezésének jelentős elterjedtsége, illetve a kötelező technikai 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 – megállapításakor, hogy az elektronikus aláírás alapját képező tanúsítvány minősített tanúsítvány-e, és azt az elektronikus aláírás készítéséhez használt biztonságos aláírás-létrehozó eszközzel társították-e az aláíráshoz.

⁽¹⁾ E nyilatkozatok tekintetében lásd az ETSI EN 319 412-5 szabványt (Elektronikus aláírások és infrastruktúrák [ESI]; Tanúsítványokat kiállító megbízható szolgáltatók profiljai; 5. rész: A minősített tanúsítványoknak megfelelő profil bővítése).

⁽²⁾ ETSI EN 319 411-2 szabvány – Elektronikus aláírások és infrastruktúrák (ESI); A tanúsítványokat kiállító megbízható szolgáltatókra vonatkozó szabályzat és biztonsági követelmények; 2. rész: Minősített tanúsítványokat kibocsátó tanúsítványkiadókra vonatkozó szabályozási követelmények.

A megbízható szolgáltatók listáján a szolgáltatásbejegyzés „szolgáltatástípus-azonosító” (Service type identifier, Sti), a „szolgáltatás neve” (Service name, Sn) és a „szolgáltatás digitális azonosítója” (Service digital identity, Sdi) mezőinek a „szolgáltatásadat-bővítmény” (Service information extensions, Sie) mező adataival való kitöltése lehetővé teszi a listán szereplő, minősített tanúsítványt kiállító hitelesítésszolgáltató hitelesítési szolgáltatása által kiállított minősített tanúsítvány konkrét típusának teljes körű meghatározását, továbbá azt, hogy adatokat tudjon szolgáltatni arról, hogy a tanúsítvány biztonságos aláírás-létrehozó eszközön alapul-e (amennyiben ez az adat a kiállított minősített tanúsítványban nem szerepel). Ehhez a bejegyzéshez külön „szolgáltatás aktuális státusa” (Service current status, Scs) adat is társul. Ez az alábbi 2. ábrán látható.

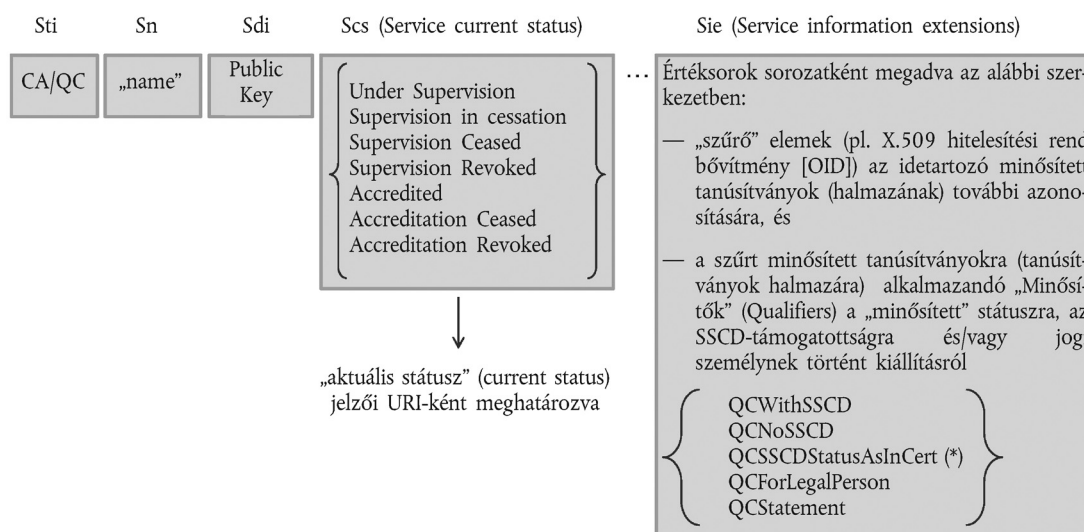
Valamely szolgáltatásnak a listán csak a legfelső szintű tanúsítványkiadó digitális azonosítójával (Sdi) való feltüntetése annyit jelent, hogy (a minősített tanúsítványt kiállító hitelesítésszolgáltató, de a hitelesítésszolgáltató felügyeletét ellátó felügyeleti/akkreditáló szerv által is) biztosított az, hogy az (ezen hierarchiában) legfelső szintű tanúsítványkiadó alatti szolgáltató által kiállított végfelhasználói tanúsítvány elegendő, az ETSI által meghatározott és géppel feldolgozható adatot tartalmaz annak értékeléséhez, hogy a tanúsítvány minősített tanúsítvány-e, és az biztonságos aláírás-létrehozó eszköz által támogatott-e. Abban az esetben például, ha ez utóbbi állítás nem igaz (pl. a minősített tanúsítványban nem szerepel ETSI szabványnak megfelelő, géppel feldolgozható jelölés arra vonatkozóan, hogy a tanúsítvány biztonságos aláírás-létrehozó eszközön alapul), és az adott legfelső szintű tanúsítványkiadónak mindössze a digitális azonosítója (Sdi) szerepel a listában, csak az feltételezhető, hogy hierarchiában a legfelső szintű tanúsítványkiadó alatti szolgáltató által kiállított minősített tanúsítványok biztonságos aláírás-létrehozó eszköz által támogatottak. Annak jelzése érdekében, hogy ezek a minősített tanúsítványok biztonságos aláírás-létrehozó eszköz által támogatottak tekintendők, a „szolgáltatásadat-bővítmény” (Sie) mezőt kell használni (ez azt is jelzi, hogy ezért az információért a minősített tanúsítványt kiállító hitelesítésszolgáltató garanciát vállal és az információt a felügyeleti vagy akkreditáló szerv felügyeleti/akkreditálja).

2. ábra

A megbízható szolgáltatók listáján szereplő, minősített tanúsítványokat kiállító hitelesítésszolgáltató szolgáltatásbejegyzése

Általános elvek – Szerkesztési szabályok – Minősített tanúsítványt kiállító hitelesítésszolgáltatók bejegyzései (listán szereplő szolgáltatások)

Szolgáltatásbejegyzések minősített tanúsítványt kiállító, listán szereplő hitelesítésszolgáltató esetén:



(*) Vagyis ez az adat szerepel az Sdi-[Sie] által meghatározott, minősített tanúsítványt kiállító hitelesítésszolgáltató tanúsítványában (ha a tanúsítványban ez nincs feltüntetve, azt jelenti, hogy SSCD által nem támogatott).

A megbízható szolgáltatók listája egységes sablonjának e technikai leírása lehetővé teszi a szolgáltatásbejegyzésben szereplő információ öt fő részének kombinálását:

- a „szolgáltatástípus azonosítója” (Service type identifier, Sti), például a minősített tanúsítványt kiállító tanúsítványkiadó azonosítására („CA/QC”),
- a „szolgáltatás neve” (Service name, Sn),
- a listába felvett szolgáltatást azonosító „szolgáltatás digitális azonosítója” (Service digital identity, Sdi) adat, például (minimálisan) a minősített tanúsítványt kiállító tanúsítványkiadó nyilvános kulcsa,

- a minősített tanúsítványt kiállító tanúsítványkiadó szolgáltatásai esetében az opcionális „szolgáltatásadat-bővítmény” (Sie) lehetővé teszi bizonyos szolgáltatásspecifikus adatok szerepeltetését a lejárt tanúsítványok visszavonási státusával, a minősített tanúsítványok további jellemzőivel, a hitelesítésszolgáltató másik hitelesítésszolgáltató általi átvételével, illetve további szolgáltatásinformációkkal kapcsolatban. A minősített tanúsítványok további jellemzőit egy vagy több értéksor sorozataként szerepelnek, ahol az egyes értéksorok az alábbiakat tartalmazzák:
 - kritériumok, melyeket a „szolgáltatás digitális azonosítójával” (Sdi) azonosított hitelesítési szolgáltatáson belül a minősített tanúsítványok egy olyan adott csoportjának további azonosítására (szűrésére) használnak, amelyek esetében további adatok szükségesek/állnak rendelkezésre a „minősített” státusra, valamint arra vonatkozóan, hogy azok biztonságos aláírás-létrehozó eszköz által támogatottak-e és/vagy azokat jogi személy részére állították-e ki, továbbá
 - az arra vonatkozó társított adatok („minősítő”), hogy a minősített tanúsítványok ezen csoportja „minősítettnek” tekinthető-e, biztonságos aláírás-létrehozó eszköz által támogatott-e, illetve hogy ez a társított adat a minősített tanúsítványnak szabványos géppel feldolgozható formában képezi-e részét, és/vagy az azt a tényt jelző adat, hogy a minősített tanúsítványt jogi személy részére állították-e ki (alapértelmezésben a tanúsítványok természetes személy részére kiállítottak minősülnek),
- a szolgáltatásbejegyzés „aktuális státus” adata, mely a következőkről ad tájékoztatást:
 - a szolgáltatás felügyelt vagy akkreditált-e, és
 - maga a felügyeleti/akkreditációs státus.

3.4. Szerkesztési és használati iránymutatás a minősített tanúsítványt kiállító hitelesítésszolgáltatók szolgáltatásbejegyzéseihez

Az **általános szerkesztési szabályok** a következők:

1. Ha (a minősített tanúsítványt kiállító hitelesítésszolgáltató által adott garancia és a felügyeleti szerv/akkreditáló szerv részéről történő felügyelet/akkreditáció révén) biztosított az, hogy a „szolgáltatás digitális azonosítójával” (Sdi) azonosított, a listán szereplő szolgáltatás esetében minden biztonságos aláírás-létrehozó eszköz által támogatott minősített tanúsítványban szerepel az ETSI által meghatározott, a minősített tanúsítvány megfelelőségére vonatkozó nyilatkozat, illetve az ETSI által meghatározott, biztonságos aláírás-létrehozó eszköz által támogatott minősített tanúsítványra vonatkozó nyilatkozat és/vagy a QCP + objektumazonosító, elegendő a megfelelő „szolgáltatás digitális azonosítója” (Sdi) mező használata, a „szolgáltatásadat-bővítmény” (Sie) mező használata pedig opcionális, és abban nem kell arra vonatkozó adatnak szerepelnie, hogy a tanúsítvány biztonságos aláírás-létrehozó eszköz által támogatott-e.
2. Ha (a minősített tanúsítványt kiállító hitelesítésszolgáltató által adott garancia és a felügyeleti szerv/akkreditáló szerv részéről történő felügyelet/akkreditáció révén) biztosított az, hogy a „szolgáltatás digitális azonosítójával” (Sdi) azonosított, a listán szereplő szolgáltatás esetében a biztonságos aláírás-létrehozó eszköz által nem támogatott minden minősített tanúsítványban szerepel a minősített tanúsítvány megfelelőségére vonatkozó nyilatkozat és/vagy a QCP + objektumazonosító, és nem szerepel a biztonságos aláírás-létrehozó eszköz által támogatott minősített tanúsítványra vonatkozó nyilatkozat vagy a QCP + objektumazonosító, elegendő a megfelelő „szolgáltatás digitális azonosítója” (Sdi) mező használata, a „szolgáltatásadat-bővítmény” (Sie) mező használata pedig opcionális, és abban nem kell arra vonatkozó adatnak szerepelnie, hogy a tanúsítvány biztonságos aláírás-létrehozó eszköz által támogatott (ami annyit jelent, hogy a tanúsítvány biztonságos aláírás-létrehozó eszköz által nem támogatott.)
3. Ha (a minősített tanúsítványt kiállító hitelesítésszolgáltató által adott garancia és a felügyeleti szerv/akkreditáló szerv részéről történő felügyelet/akkreditáció révén) biztosított az, hogy az „szolgáltatás digitális azonosítójával” (Sdi) azonosított, a listán szereplő szolgáltatás esetében minden minősített tanúsítványban szerepel a minősített tanúsítvány megfelelőségére vonatkozó nyilatkozat és e tanúsítványok egy része biztonságos aláírás-létrehozó eszköz által támogatottak, egy másik része pedig nem (ilyen megkülönböztetés a hitelesítésszolgáltató egyedi hitelesítési rend objektumazonosítására vagy más, a hitelesítésszolgáltatóra jellemző adat révén magában a minősített tanúsítványban is tehető, közvetlenül vagy közvetetten, géppel feldolgozható formában vagy másként), de a biztonságos aláírás-létrehozó eszköz által támogatott tanúsítványban nem szerepel SEM a biztonságos aláírás-létrehozó eszköz által támogatott minősített tanúsítványra vonatkozó nyilatkozat, SEM az ETSI QCP(+) objektumazonosító, nem feltétlenül elegendő a megfelelő „szolgáltatás digitális azonosítója” (Sdi) mező használata, ÉS a „szolgáltatásadat-bővítmény” (Sie) mezőt kell használni azon adat kifejezett megadására, hogy a tanúsítvány biztonságos aláírás-létrehozó eszköz által támogatott-e, az ide tartozó tanúsítványcsoportok azonosítására használt esetleges adatbővítményekkel együtt. Ez a „szolgáltatásadat-bővítmény” (Sie) mező igénybevételekor valószínűleg különböző, „a biztonságos aláírás-létrehozó eszközzel való támogatottságot kifejező értékek” (SSCD support information values) felvételét teszi szükségessé ugyanazon „szolgáltatás digitális azonosító” (Sdi) esetében.
4. Ha (a minősített tanúsítványt kiállító hitelesítésszolgáltató által adott garancia és a felügyeleti szerv/akkreditáló szerv részéről történő felügyelet/akkreditáció révén) biztosított az, hogy a „szolgáltatás digitális azonosítójával” (Sdi) azonosított, a listán szereplő szolgáltatás esetében egy minősített tanúsítványban sem szerepel a minősített tanúsítvány megfelelőségére vonatkozó nyilatkozat, a QCP objektumazonosító, a biztonságos aláírás-létrehozó eszköz által támogatott minősített tanúsítványra vonatkozó nyilatkozat vagy a QCP + objektumazonosító, de biztosított, hogy a „szolgáltatás digitális azonosítója” (Sdi) alapján kiállított végfelhasználói tanúsítványok egy részét minősített tanúsítványnak és/vagy biztonságos aláírás-létrehozó eszköz által támogatottnak szánták, egy másik részét pedig nem (ilyen megkülönböztetés a minősített tanúsítványt kiállító hitelesítésszolgáltató egyedi hitelesítési rend objektumazonosítója vagy más, a minősített tanúsítványt kiállító hitelesítésszolgáltatóra jellemző adat révén magában a minősített tanúsítványban is tehető, közvetlenül vagy közvetetten, géppel feldolgozható formában vagy másként), nem elegendő a megfelelő „szolgáltatás digitális azonosítója” (Sdi) mező használata, ÉS a „szolgáltatásadat-bővítmény” (Sie) mezőt kell használni a minősítésre vonatkozó adat kifejezett megadására. Ez a „szolgáltatásadat-bővítmény” (Sie) mező igénybevételekor valószínűleg különböző, „a biztonságos aláírás-létrehozó eszközzel való támogatottságot kifejező értékek” (SSCD support information values) felvételét teszi szükségessé ugyanazon „szolgáltatás digitális azonosító” (Sdi) esetében.

Általános alapértelmezett elvként a megbízható szolgáltatók listájára felvett hitelesítésszolgáltatók esetében minden egyes nyilvános kulcshoz egy szolgáltatásbejegyzésnek kell tartoznia a CA/QC típusú hitelesítési szolgáltatás esetén, azaz a

minősített tanúsítványt (közvetlenül) kiállító hitelesítésszolgáltató esetében. Bizonyos kivételes körülmények esetében és gondosan irányított feltételek mellett a tagállami felügyeleti/akkreditáló szerv dönthet úgy, hogy a listán szereplő hitelesítésszolgáltató szolgáltatáslistájának valamely egyszeri bejegyzésének „szolgáltatás digitális azonosítójaként” (Sdi) a legfelső vagy felső szintű tanúsítványkiadónak a hitelesítésszolgáltató nyilvános kulcsú infrastruktúrájához tartozó nyilvános kulcsát használja (például a hitelesítésszolgáltatónak a legfelső szintű tanúsítványkiadótól a többi tanúsítványkiadóig terjedő hierarchiával összefüggésében) az összes alárendelt tanúsítványkiadó szolgáltatásának felsorolása helyett (azaz a végfelhasználói tanúsítványok közvetlen kiállításával nem foglalkozó, de a tanúsítványkiadók hierarchiáját a végfelhasználóknak minősített tanúsítványt kiállító tanúsítványkiadókkal bezárólag hitelesítő szolgáltatót szerepelteti a listán). Alkalmazása esetén a tagállamoknak körültekintően mérlegelniük kell a legfelső vagy felső szintű tanúsítványkiadó nyilvános kulcsának a megbízható szolgáltatók listáján a „szolgáltatás digitális azonosítójaként” (Sdi) történő használata következményeit (előnyeit és hátrányait). Emellett, az alapértelmezett elvtől való ezen engedélyezett kivétel alkalmazásakor a tagállamnak át kell adnia a hitelesítési útvonal felépítését és ellenőrzését lehetővé tevő szükséges dokumentációt. Azon minősített tanúsítványt kiállító hitelesítésszolgáltatók esetében például, amelyek olyan egyetlen legfelső szintű tanúsítványkiadót használnak, amely alatt több tanúsítványkiadó állít ki minősített és fokozott biztonságú tanúsítványokat, de amelyek esetében a minősített tanúsítványokban csak a minősített tanúsítvány megfelelőségére vonatkozó nyilatkozat szerepel, és az nem tünteti fel, hogy a tanúsítvány biztonságos aláírás-létrehozó eszköz által támogatott-e, a legfelső szintű tanúsítványkiadó „szolgáltatás digitális azonosítójának” (Sdi) listán való feltüntetése csak annyit jelent – a fent kifejtett szabályok értelmében –, hogy az ebben a legfelső szintű tanúsítványkiadó alatti hierarchiában kiállított tanúsítványok egyike sem támogatott biztonságos aláírás-létrehozó eszköz által. Ha vannak olyan minősített tanúsítványok, amelyek ténylegesen biztonságos aláírás-létrehozó eszköz által támogatottak, de géppel feldolgozható nyilatkozat nem jelzi, hogy a tanúsítványoknak ez a támogatottság is része lenne, a jövőben kiállított minősített tanúsítványokra nézve nyomatékosan ajánlott a biztonságos aláírás-létrehozó eszközön alapuló minősített tanúsítványra vonatkozó nyilatkozat igénybevétele. Ezzel egyidejűleg (az ezen információt nem tartalmazó utolsó minősített tanúsítvány lejártáig) a megbízható szolgáltatók listáján igénybe kell venni a „szolgáltatásadat-bővítmény” és a hozzá kapcsolódó „minősítésbővítmény” (Qualifications Extension) mezőt például szűrési adatokat adva meg a minősített tanúsítványokat kiállító hitelesítésszolgáltató által meghatározott azon objektumazonosítókra keresztül, amelyeket a minősített tanúsítványokat kiállító hitelesítésszolgáltató potenciálisan a különböző típusú minősített tanúsítványok megkülönböztetésére használ (amelyek egy része biztonságos aláírás-létrehozó eszköz által támogatott, egy másik része pedig nem támogatott) és a „minősítők” használatán keresztül kifejezetten „biztonságos aláírás-létrehozó eszköz által támogatott” információt társítva a (kiszűrt) tanúsítványcsoport(ok)hoz.

Az ezen technikai leírásnak megfelelő megbízható szolgáltatók listáján alapuló elektronikus aláírási alkalmazások, szolgáltatások vagy termékek esetében a következő **általános használati iránymutatások** érvényesülnek:

A „CA/QC” „Sti” bejegyzés (valamint a „Sie” additionalServiceInformation [szolgáltatás további adatai] bővítménnyel „RootCA/QC”-ként [gyökértanúsítvány-kiállítási szolgáltatásként] tovább minősített CA/QC bejegyzés)

- jelzi, hogy az „Sdi” által azonosított tanúsítványkiadótól (és ugyanígy az „Sdi” által azonosított legfelső szintű tanúsítványkiadóval kezdődő szolgáltatói hierarchiából) származó, valamennyi kiállított végfelhasználói tanúsítvány minősített tanúsítvány, feltéve, hogy ez a megfelelő minősített tanúsítványra vonatkozó, géppel feldolgozható nyilatkozat (azaz a minősített tanúsítvány megfelelőségére vonatkozó nyilatkozat) és/vagy az ETSI által meghatározott QCP(+) objektumazonosítók használata útján szerepel magában a tanúsítványban (és ezt a felügyeleti/akkreditáló szerv biztosítja, lásd fentebb az „általános szerkesztési szabályok”).

Megjegyzés: ha nem szerepel „Sie” „minősítésbővítmény” (Qualifications Extension) adat, vagy ha valamely minősített tanúsítványként feltüntetett végfelhasználói tanúsítvány nem azonosítható pontosabban valamely kapcsolódó „Sie” „minősítésbővítmény” bejegyzés révén, a minősített tanúsítványban található „géppel feldolgozható” adat helyessége felülvizsgált/akkreditált. Ez annyit jelent, hogy a megfelelő minősített tanúsítványra vonatkozó nyilatkozatok (azaz a minősített tanúsítvány megfelelőségére vonatkozó nyilatkozat, a 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,

- és HA szerepel a „Sie” „minősítésbővítmény” adat, a fenti alapértelmezett használati szabályon túlmenően azokat a tanúsítványokat, amelyeket ezen – a tanúsítványcsoportok további azonosítására szolgáló „szűrők” sorozata elvén létrehozott – „Sie” „minősítésbővítmény” bejegyzés használata révén azonosítanak, a minősített státusra, „a biztonságos aláírás-létrehozó eszközzel való támogatottságra” (SSCD support) és/vagy a „jogi személy címet” (Legal person as subject) tényére vonatkozóan további adatokat is szolgáltató kapcsolódó minősítőknél megfelelően kell vizsgálni (például a hitelesítési rend bővítményben egyedi objektumazonosítókat tartalmazó és/vagy egyedi „fő felhasználás” tulajdonságokkal rendelkező tanúsítványok, és/vagy egy adott tanúsítványmezőben vagy bővítményben megjelenő egyedi érték használatával szűrt tanúsítványok stb.). Ezek a minősítők a „minősítők” alábbi, az érintett minősített tanúsítvány adathiányát kompenzáló csoportjába tartoznak, amelyeket az alábbiakra használnak:

- a minősített státus jelölése: „QCStatement”, amely azt jelenti, hogy az adott tanúsítvány(ok) minősített(ek),

ÉS/VAGY

- a biztonságos aláírás-létrehozó eszközzel való támogatottság jellegének jelzése:

- „QCWithSSCD” minősítő érték, amelynek jelentése: „QC supported by an SSCD” (a minősített tanúsítvány biztonságos aláírás-létrehozó eszköz által támogatott), vagy
- „QCNoSSCD” minősítő érték, amelynek jelentése „QC not supported by an SSCD” (a minősített tanúsítvány biztonságos aláírás-létrehozó eszköz által nem támogatott), vagy
- „QCSSCDStatusAsInCert” minősítő érték, amelynek jelentése, hogy a biztonságos aláírás-létrehozó eszközzel való támogatottságra vonatkozó adat biztosan szerepel minden minősített tanúsítványban ezen minősített tanúsítványt kiállító tanúsítványkiadó (CA/QC) „Sdi”-„Sie” mezőjében,

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).

3.5. A minősített tanúsítványokat kiállító tanúsítványkiadó (CA/QC) szolgáltatásait támogató, de a CA/QC digitális azonosítójának (Sdi) részét nem képező szolgáltatások

A minősített tanúsítványok és azon tanúsítványok érvényességi státusával kapcsolatos szolgáltatásokat, amelyekre vonatkozóan az érvényességi státusra vonatkozó adatot (pl. tanúsítvány-visszavonási listák és valós idejű tanúsítvány-lekérdezésekre adott válaszok) olyan szervezet írja alá, amelynek titkos kulcsa nincs minősített tanúsítványokat kiállító, a listán szereplő tanúsítványkiadó által hitelesítve, a megbízható szolgáltatók listáján a tanúsítvány érvényességi státusával kapcsolatos szolgáltatások felsorolása útján kell a listán szerepeltetni (azaz minősített tanúsítványokhoz kapcsolódó „valós idejű tanúsítvány-lekérdezések” [OCSP/QC] vagy „tanúsítvány-visszavonási listák” [CRL/QC] szolgáltatástípus bejegyzéssel), hiszen ezek a szolgáltatások a minősített tanúsítványokhoz kapcsolódó hitelesítési szolgáltatások részét képező felügyelt/akkreditált „minősített” szolgáltatásoknak tekinthetők. Természetesen úgy kell tekinteni, hogy azok a valós idejű tanúsítványlekerdezés-válaszadó egységek vagy tanúsítványvisszavonáslista-kiadók, amelyek tanúsítványait a minősített tanúsítványkiállítási szolgáltatások hierarchiájába bejegyzett tanúsítványkiadók írják alá, „érvényes” (valid) státusszal rendelkeznek és megfelelnek a listán szereplő minősített tanúsítványkiállítási szolgáltatás státusértékének.

Hasonló rendelkezés vonatkozhat a („CA/PKC” szolgáltatástípusú) fokozott biztonságú tanúsítványokat kiállító hitelesítési szolgáltatásokra.

A megbízható szolgáltatók listáján szerepeltetni kell a tanúsítványok érvényességi státusával kapcsolatos szolgáltatásokat, amennyiben a tanúsítvány érvényességi státusával kapcsolatos szolgáltatás által érintett végfelhasználói tanúsítványokban nem szerepel az ezen szolgáltatások elérhetőségével kapcsolatos információ.

4. Fogalommeghatározások és rövidítések

Ebben a dokumentumban a következő fogalommeghatározásokat és betűszavakat használjuk:

Kifejezés	Betűszó	Meghatározás
Hitelesítésszolgáltató	CSP	Az 1999/93/EK irányelv 2. cikkének 11. pontjában szereplő fogalommeghatározás szerint
Tanúsítványkiadó	CA	1. nyilvános kulcsú tanúsítványokat létrehozó és kiosztó hitelesítésszolgáltató; vagy 2. technikai tanúsítvány-előállító szolgáltatás, amelyet valamely nyilvános kulcsú tanúsítványokat létrehozó és kiosztó hitelesítésszolgáltató vesz igénybe. <i>Megjegyzés:</i> A tanúsítványkiadó fogalmának részletesebb magyarázatáért lásd az EN 319 411-2 szabvány (!) 4. pontját.
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	Az 1999/93/EK irányelv 2. cikkének 9. pontjában szereplő fogalommeghatározás szerint.
Minősített tanúsítvány	QC	Az 1999/93/EK irányelv 2. cikkének 10. pontjában szereplő fogalommeghatározás szerint.
Aláíró	Aláíró	Az 1999/93/EK irányelv 2. cikkének 3. pontjában szereplő fogalommeghatározás szerint.
Felügyelet	Felügyelet	Az 1999/93/EK irányelv 3. cikkének (3) bekezdésében előírt felügyelet. Az 1993/93/EK irányelv olyan megfelelő rendszer kialakítását írja elő a tagállamok számára, amely lehetővé teszi a területükön letelepedett és a 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. pontjában 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.

Kifejezés	Betűszó	Meghatározás
Megbízhatósági állapot-lista	TSL	A megbízhatósági állapotadatok ETSI TS 119 612 szabványban meghatározott előírások szerinti bemutatására használt, aláírt lista.
Megbízhatósági szolgáltatás		Az elektronikus ügyletekbe vetett bizalom és az ügyletek megbízhatóságának fokozását szolgáló szolgáltatás (amely rendszerint, de nem szükségszerűen titkosítási technikákat használ vagy bizalmas anyagokra vonatkozik) (ETSI TS 119 612 szabvány). Megjegyzés: A fogalom a tanúsítványok kiállítását vagy az elektronikus aláírásokkal kapcsolatos egyéb szolgáltatások nyújtását magában foglaló hitelesítési szolgáltatásnál tágabb értelmezésben használt.
Megbízható szolgáltató	TSP	Egy vagy több (elektronikus) megbízhatósági szolgáltatást működtető szervezet. (A fogalom a hitelesítésszolgáltató fogalmánál tágabb értelemben használt.)
Megbízhatóságszolgáltatás-token	TrST	Megbízhatósági szolgáltatás igénybevétele nyomán létrejövő vagy kiállított fizikai vagy bináris (logikai) objektum. Bináris megbízhatóságszolgáltatás-tokenek például a tanúsítványok, a tanúsítvány-visszavonási listák (CRL), az időbélyegzők és a valós idejű tanúsítványlekérdezésre (OCSP) adott válaszok.
Minősített elektronikus aláírás	QES	Minősített tanúsítvánnyal támogatott fokozott biztonságú elektronikus aláírás, amelyet 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. pontjában szereplő fogalom meghatározás szerint.
Minősített tanúsítvánnyal támogatott fokozott biztonságú elektronikus aláírás	AdES _{QC}	Olyan elektronikus aláírás, mely megfelel a fokozott biztonságú elektronikus aláírások követelményeinek, és amely az 1999/93/EK irányelv 2. cikkében meghatározott minősített tanúsítvány által támogatott.
Biztonságos aláírás-létrehozó eszköz	SSCD	Az 1999/93/EK irányelv 2. cikkének 6. pontjában szereplő fogalom meghatározás szerint.

(¹) EN 319 411-2 szabvány; Elektronikus aláírások és infrastruktúrák (ESI); A tanúsítványokat kiállító megbízható szolgáltatókra vonatkozó szabályozási és biztonsági követelmények; 2. rész: Minősített tanúsítványokat kibocsátó tanúsítványkiadókra (CA/QC) vonatkozó szabályozási követelmények.

A dokumentum következő fejezeteiben 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 leírtak irányadók (¹).

I. FEJEZET

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

Ez a leírás az ETSI TS 119 612 v1.1.1. szabványban (a továbbiakban: ETSI TS 119 612 szabvány) szereplő leíráson és követelményeken alapul.

Amennyiben a leírás különleges követelményt nem tartalmaz, teljes mértékben az ETSI TS 119 612 szabvány 5. és 6. pontját KELL alkalmazni. Amennyiben a leírás különleges követelményeket tartalmaz, ezeknek elsőbbséget KELL élvezniük az ETSI TS 119 612 szabvány vonatkozó követelményeivel szemben. A leírás és az ETSI TS 119 612 szabvány leírása közötti eltérés esetén e leírást KELL irányadónak tekinteni.

Scheme operator name (Rendszerüzemeltető neve) (5.3.4. pont)

Ennek a mezőnek szerepelnie KELL és meg KELL felelnie az ETSI TS 119 612 szabvány 5.3.4. pontjában meghatározott követelményeknek.

(¹) IETF RFC 2119: „Key words for use in RFCs to indicate Requirements Levels”. (A követelményszintek jelzésére az RFC-ben alkalmazandó kulcsszavak.)

Az országoknak bármely kapcsolódó operatív tevékenység vonatkozásában elkülönült felügyeleti és akkreditációs szervei is LEHETNEK. Az egyes tagállamok feladata a megbízható szolgáltatók tagállami listája rendszerüzemeltetőjének kijelölése. 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 történő megjelölést is.

Scheme name (Rendszer neve) (5.3.6. pont)

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

„EN_name_value” = „A rendszerüzemeltető tagállam által az elektronikus aláírásra vonatkozó közösségi keretfeltételekről szóló, 1999. december 13-i 1999/93/EK európai parlamenti és tanácsi irányelvben megállapított vonatkozó rendelkezéseknek való megfelelés tekintetében felügyelt/akkreditált hitelesítésszolgáltatók hitelesítési szolgáltatásainak felügyeleti/akkreditációs státuslistája”.

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

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

- Általános bevezető adatok, amelyek a megbízható szolgáltatók listájának alkalmazási köre és kontextusa tekintetében valamennyi tagállam esetében azonosak, valamint az alkalmazott felügyeleti/akkreditációs rendszer(ek). Az azonos szövegrész az alábbi szöveg, amelyben „[name of the relevant member state]” (az érintett tagállam neve) szövegrészt az érintett tagállam nevével KELL helyettesíteni:

„The present list is the „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;
- allowing for a trusted validation of electronic signatures supported by those listed supervised/ accredited certification services from the listed CSPs.

The Trusted List of a Member State provides, as a minimum, information on supervised/ accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3) and Article 7(1)(a)), including, when this is not part of the QCs, 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 compliance 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 Article 3(3), Article 8.(1), Article 11 (respectively, Article 2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 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 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,
 - 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 alkalmazott 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 „minősítések” (qualifications) – amely minősítéseket a nemzeti szinten megállapított rendelkezések és követelmények teljesítése alapján adnak meg – külön adatai, ideértve a „minősítés” jelentését és a kapcsolódó nemzeti rendelkezéseket és követelményeket.

A rendszerre vonatkozó további tagállamspecifikus adatokat önkéntes alapon LEHET megadni. Ilyen adat lehet például:

- a felügyelők/auditorok kiválasztásra használt szempontok és szabályok, valamint a hitelesítésszolgáltatók vonatkozásában általuk gyakorolt felügyelet (ellenőrzés)/akkreditáció (audit) meghatározása,
- a rendszer üzemeltetésére vonatkozó egyéb kapcsolattartási és általános adatok.

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

Ennek a mezőnek szerepelnie KELL és meg KELL felelnie az ETSI TS 119 612 szabvány 5.3.9. pontjában meghatározott követelményeknek, és legalább két URI-t KELL tartalmaznia:

- A megbízható szolgáltatók valamennyi tagállami listája tekintetében azonos URI, amely olyan leíró szövegre mutat, amelynek a megbízható szolgáltatók összes listájára KELL vonatkoznia, az alábbiak szerint:

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

Leíró szöveg:

„Participation in a scheme

Each Member State must create a „Trusted List 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 implementation of such Trusted Lists is also to be referred to in the list of links (pointers) towards each Member State’s Trusted List, compiled by the European Commission.

Policy/rules for the assessment of the listed services

The Trusted List of a Member State must provide, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3) and Article 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.

⁽¹⁾ Az utolsó két adatcsoport kulcsfontosságú a listát használók számára a minősített tanúsítvány kiállításával nem foglalkozó hitelesítésszolgáltatókra alkalmazott felügyeleti/akkreditációs rendszerek minőségének és biztonsági szintjének értékeléséhez. Ezeket az adatcsoportokat a megbízható szolgáltatók listája szintjén kell megadni, „a rendszer adatainak URI-ja” (Scheme information URI) (5.3.7. pont – tagállamok által megadott adatok), a „rendszer típus/közösség/szabályok” (Scheme type/community/rules) (5.3.9. pont – valamennyi tagállam esetében azonos szöveggel, és a tagállam által megadott, nem kötelező adatok révén) és a „megbízhatósági állapotlista szabályzat/jogi nyilatkozat” (TSL policy/legal notice) (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 rendszer szolgáltatásai meghatározásának URI-ja” (Scheme service definition URI) (5.5.6. pont) mező használatával.

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 compliance 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 Article 3(3), Article 8(1), Article 11 (respectively, Article 2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 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 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 Article 2(11) of Directive 1999/93/EC). 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 Trusted List

The **general user guidelines** for electronic signature applications, services or products relying on a Trusted List according to the Annex of Commission Decision [reference to the present Decision] 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 EN 319 412-5 defined QcStatements (i.e. QcCompliance, QcSSCD, etc.) and/or EN 319 411-2 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

Note: if no „Sie" „Qualifications Extension" information is present or if an end-entity certificate that is claimed to be a QC is not further identified through a related „Sie" „Qualifications Extension" information, 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. QcCompliance, QcSSCD, etc.) 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" „Qualifications Extension" information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this „Sie" „Qualifications Extension" information, 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 the qualified status, the „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 qualified status: „QCStatement" meaning the identified certificate(s) is(are) qualified,

AND/OR

— 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/EC for further details on the fields, description and meaning for the Member States’ Trusted Lists.”

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

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

- Ahol a felhasználók elérhetik az adott tagállam azon egyedi szabályzatát/szabályait, amelyek alapján a listán szereplő szolgáltatásokat értékelni KELL a tagállam megfelelő felügyeleti rendszerének és önkéntes akkreditációs rendszerének megfelelően.
- Ahol a felhasználók elérhetik az adott tagállamra vonatkozó külön leírásokat arról, hogy miként kell a megbízható szolgáltatók listájának a minősített tanúsítványok kiállításával nem összefüggő hitelesítési szolgáltatásokkal kapcsolatos tartalmát használni és értelmezni. Ez a minősített tanúsítványok kiadásával nem foglalkozó hitelesítés-szolgáltatók nemzeti felügyeleti/akkreditációs rendszerek potenciális granularitásának és annak a jelzésére használható, hogy „a rendszer szolgáltatásai meghatározásának URI-ja” (Scheme service definition URI) (5.5.6. pont) és a „szolgáltatásadat-bővítmény” (Service information extension) (5.5.9. pont) mezőket miként használják erre a célra.

A tagállamoknak további URI-kat LEHET meghatározniuk és használniuk a fenti tagállamspecifikus URI-kból (azaz a specifikus URI-k hierarchiájából meghatározott URI-kat).

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

Ennek a mezőnek szerepelnie KELL és meg KELL felelnie az ETSI TS 119 612 szabvány 5.3.11. pontjában meghatározott követelményeknek, továbbá a rendszer jogi státusára vonatkozó szabályzatnak/jogi nyilatkozatnak vagy a rendszer létrehozása helyének megfelelő joghatóság szerinti, a rendszer által teljesített jogi követelményeknek és/vagy bármilyen korlátozásnak és feltételnek, amely a megbízható szolgáltatók listájának vezetésére és közzétételére vonatkozik, többnyelvű karaktorsorozatnak (sima szöveg) KELL lennie, amely két részből áll:

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

Az azonos 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 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.”

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

A közös szöveg magyar nyelvi változata:

„A [az érintett 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] joga szerinti végrehajtási rendelkezések.”

2. A második, a megbízható szolgáltatók egyes tagállami listáira vonatkozó opcionális rész (kötelező nyelvként egyesült királyságbeli angol nyelven és esetlegesen egy vagy több nemzeti nyelven) feltünteti az irányadó nemzeti jogszabályi keretre vonatkozó információkat (például ha az a minősített tanúsítvány kiállításával nem foglalkozó hitelesítés-szolgáltatók nemzeti felügyeleti/akkreditációs rendszereihez kapcsolódik).

II. FEJEZET

A MEGBÍZHATÓ SZOLGÁLTATÓK LISTÁINAK FOLYAMATOSSÁGA

Az ezen határozat 3. cikkének c) pontja alapján a Bizottságnak bejelentendő tanúsítványokat úgy KELL kiállítani, hogy:

- érvényességük kezdete és vége között legalább három hónap legyen,
- új kulcspárok alapján hozzák létre őket, mivel korábban már használt kulcspár újból nem hitelesíthető.

A nyilvános kulcshoz tartozó, a megbízható szolgáltatók listája aláírásának érvényesítésére használható, a Bizottságnak bejelentett és a Bizottság által a hivatkozásokról vezetett központi listán közzétett titkos kulcsok EGYIKÉNEK kompromittálódása vagy visszavonása esetén a tagállamoknak a következőket KELL tenniük:

- amennyiben a közzétett listát kompromittálódott vagy visszavont titkos kulccsal írták alá, haladéktalanul újból kiállítják a megbízható szolgáltatók új, nem kompromittálódott titkos kulccsal aláírt listáját,
- azonnal tájékoztatják a Bizottságot a megbízható szolgáltatók listájának aláírására használható titkos kulcsokhoz tartozó nyilvános kulcsú tanúsítványok új listájáról.

A nyilvános kulcshoz tartozó, a megbízható szolgáltatók listája aláírásának érvényesítésére használható, a Bizottságnak bejelentett és a Bizottság által a hivatkozásokról vezetett központi listán közzétett titkos kulcsok MINDEGYIKÉNEK kompromittálódása vagy visszavonása esetén a tagállamoknak a következőket KELL tenniük:

- új kulcspárokat generálnak, amelyekkel a megbízható szolgáltatók listája és a hozzájuk tartozó nyilvános kulcsú tanúsítványok aláírhatók,
- haladéktalanul újból kiállítják a megbízható szolgáltatók új listáját, amelyet az új titkos kulcsok valamelyikével írtak alá és az amelyhez tartozó nyilvános kulcsú tanúsítványokról értesítést kell küldeniük,
- azonnal tájékoztatják a Bizottságot a megbízható szolgáltatók listájának aláírására használható titkos kulcsokhoz tartozó nyilvános kulcsú tanúsítványok új listájáról.

III. FEJEZET

LEÍRÁS A MEGBÍZHATÓ SZOLGÁLTATÓK LISTÁJÁNAK EMBERI SZEMMEL OLVASHATÓ FORMÁJÁHOZ

Amennyiben létrehozták és közzétették a megbízható szolgáltatók listájának emberi szemmel olvasható formáját, azt az ISO 32000 szabványnak ⁽¹⁾ megfelelő Portable Document Format (PDF) dokumentum formájában JAVASOLT elkészíteni, és annak formátumát a PDF/A (ISO 19005) profilnak ⁽²⁾ megfelelően KELL kialakítani.

A megbízható szolgáltatók listája PDF/A-alapú, emberi szemmel olvasható formájának a következő követelményeknek JAVASOLT megfelelnie:

- Az emberi szemmel olvasható forma felépítésének az ETSI TS 119 612 szabványban 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) (pl. „Nyilvános kulcsú tanúsítványokat kiállító tanúsítványkiadó”),
 - adott esetben több természetes nyelvi változat, a megbízható szolgáltatók listájában előírtak szerint.

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

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

- Legalább a „szolgáltatás digitális azonosítója” (Sdi) mezőben szereplő digitális tanúsítványok következő mezőit és megfelelő értékeit JAVASOLT az emberi szemmel olvasható formában megjeleníteni:
 - Verzió
 - Sorozatszám
 - Aláíró algoritmus (Signature algorithm)
 - Kiállító (Issuer)
 - Érvényesség kezdete
 - Érvényesség vége
 - Tulajdonos (Subject)
 - 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 formát a rendszerüzemeltetőnek a PAdES Signatures baseline profile-nak ⁽¹⁾ megfelelően KELL aláírnia.
-

⁽¹⁾ ETSI TS 103 172 szabvány (2012. március) – Elektronikus aláírások és infrastruktúrák (ESI); PAdES Baseline Profile.