MÁV INFORMATIKA

Kereskedelmi, Szolgáltató és Tanácsadó Kft.

Nyilvános körben kibocsátott minősített tanúsítványtípusra (MTT) érvényes Hitelesítési Politika

Verziószám	**1.1**
Jóváhagyás dátuma	**2003. március 31.**

MÁV INFORMATIKA Kereskedelmi, Szolgáltató és Tanácsadó Kft.
1012 Budapest, Krisztina krt. 37/a., 1253 Budapest Pf. 28. Tel.: 457-9300, fax: 457-9500,
e-mail: mavinformatika@mavinformatika.hu

ISO 9001:2000
NYILVÁNTARTÁSI SZÁM: 503/0660

A dokumentum neve	Nyilvános körben kibocsátott minősített tanúsítvány-típusra (MTT) érvényes Hitelesítési Politika (HP) *
HP verziószám	1.1
Üzemelő PKI szoftver verziószám (Technikai azonosító)	Trust&Sign QCAV1.0
Hírközlési Felügyelet regisztrációs szám	
HP objektum azonosító (OID)	1.3.6.1.4.1.14868.2.2.1
Első hatálybalépés időpontja	2002. 12. 20.
Aktuális változat hatálybaléptetés időpontja	2003. 03. 31.
Következő felülvizsgálat időpontja:	2003. 06. 31.

	Név	**Szervezeti egység**	**Aláírás**	**Dátum**
Készítette:	Bodlaki Ákos	QCA projekt		2002. 12. 08.
Ellenőrizte:	Tóth Elemér	QCA Projekt		2003. 01. 30.
Ellenőrizte:	Tóth Elemér	QCA Projekt		2003. 03. 30.
Jóváhagyta:	Dombai Ferenc	vezérigazgató		2003. 03. 31.

* A MÁV INFORMATIKA Kft. nyilvános körben kibocsátott minősített tanúsítványtípusra (MTT) érvényes Hitelesítési Politikája az Internet Közösség RFC 2527 ajánlásában és az EU ETSI TS 101 456 szabványában javasolt Certificate Policy (CP) szerkezetet követi. A *Hitelesítési Politika* fogalom megfelel hazai joganyag szerinti *tanúsítványtípus*, illetve a nemzetközi ajánlások, szabványok szerinti *Certificate Policy* elnevezésnek.

HP verziók

Verzió	Dátum	A változás leírása	Hatálybalépés dátuma	Készítette
1.0	2002. 12. 08	A nyilvános körben kibocsátott minősített tanúsítványtípus (MTT) szolgáltatói minősítésére előkészített változat.		Bodlaki Ákos
1.1	2003. 01. 28	A minősítési eljárásra átadott változat		Bodlaki Ákos, Benkó Tamás, Tóth Elemér, Vész Ferenc
1.1	2003. 03. 31	A minősítési eljárásra jóváhagyott változat		Bodlaki Ákos, Tóth Elemér

TARTALOMJEGYZÉK

1. Bevezetés

E dokumentum a MÁV INFORMATIKA Kft. (továbbiakban Szolgáltató) elektronikus hitelesítés szolgáltatása keretében kibocsátott Aláírás létrehozó adatok hitelességét bizonyító tanúsítványok kezelésére (előállítás, felfüggesztés, visszavonás, megújítás) vonatkozó eljárásrendet, a tanúsítványok szerkezetét, a tanúsítványok tartalmának és érvényességének ellenőrzési eljárásait és az egyéb működési szabályokat tartalmazza.

A Szolgáltató a hitelesítés szolgáltatást a vele előfizetői szerződéses viszonyban álló partnerek, valamint az aláírások hitelességét ellenőrző érintett felek részére szolgáltatja.

A jelen Hitelesítési Politikát a következők használják:

- a Szolgáltató személyzete, annak érdekében, hogy a szolgáltatási tevékenység a hatályos jogszabályokkal és a Szolgáltató belső szabályzataival összhangban valósuljon meg,
- az ellenőrző hatóságok,
- a belső és külső auditorok.

Az elektronikus hitelesítés szolgáltatások keretében a Szolgáltató a vele szerződéses kapcsolatban álló aláírók részére a 2001. évi XXXV. törvényben meghatározott szolgáltatások közül a következőket nyújtja:

- elektronikus aláírás hitelesítés szolgáltatás,
- Aláírás létrehozó eszközön az Aláírás létrehozó adat elhelyezése.

Ezen szolgáltatásokat a Szolgáltató fokozott biztonságú szinten szolgáltatja.

A Hitelesítési Politika (továbbiakban: HP) jelen aktuális verziója a PKI alkalmazás mindenkori technikai azonosítójával van összerendelve, azaz a HP-ben foglaltak a technikai azonosítóval azonosított PKI alkalmazásra vonatkoznak.

Az aktuális PKI alkalmazás technikai azonosító*:* Trust&Sign QCAV1.0

1.1. Áttekintés

1.1.1. Szabályzat célja

A HP egy olyan szabálygyűjtemény, mely egy Tanúsítvány felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára, valamint meghatározza azokat a követelményeket, amelyeket a Szolgáltatónak a tanúsítvány kezelés folyamatában teljesítenie kell.

A szabályokra vonatkozó követelmények jelen dokumentumban a nyilvános körben kibocsátott minősített tanúsítványtípusra (MTT) vonatkoznak.

A tanúsítványok végfelhasználóinak tevékenységére vonatkozóan jelen HP-től független egyéb belső szabályzatok is élhetnek előírásokkal. Amennyiben e szabályzatok bármely vonatkozásban ellentmondást vagy eltérő kikötést tartalmaznának, jelen HP előírásai tekinthetők magasabb szintűnek, s ezek alkalmazandók.

1.1.2. Jogszabályok, szabványok, ajánlások

A jelen HP a következő jogszabályokat, szabványokat, és ajánlásokat vesz figyelembe

a HP teljes tartalmára vonatkozóan:

- 2001. évi XXXV. törvény az elektronikus aláírásról,
- 2/2002. (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről.
- 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről,
- ISO/IEC 15408 1999: Információ technológia - Biztonsági módszerek - Informatikai biztonság értékelési kritériumai (1-3 részek),

a HP szerkezetére és tartalmára vonatkozóan:

- RFC 2527 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és szolgáltatási szabályzat keretrendszer),
- Hírközlési Felügyelet minta szabályzata „Minősített tanúsítványtípus minták minősített hitelesítés-szolgáltatók számára" címmel,

a tanúsítványokra, visszavonási listák szerkezetére, tartalmára vonatkozóan:

- ITU-T X.509 "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks" ajánlás 3. verziója,

- RFC 2459 (Internet X.509 Nyilvános kulcsú infrastruktúra – Tanúsítvány és Tanúsítvány visszavonási lista profil)

a hitelesítés szolgáltatásra és a szolgáltatókra vonatkozóan:

- 2001. évi XXXV. törvény az elektronikus aláírásról,
- 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről,
- 151/2001. (IX. 1.) Korm. rendelet a Hírközlési Felügyeletnek az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásaának részletes szabályairól,

informatikai biztonsági követelmények: MeH 12. ajánlás, ITSEC[2], CC[3],

az Aláírás létrehozó eszközre vonatkozóan:

- NIST FIPS PUB 140-1 (1994. január 11) (Kriptográfiai modulok biztonsági követelményei),
- CEN 14167-2 munkacsoport egyezmény: „Védelmi profil hitelesítés-szolgáltató aláíró műveleteit megvalósító kriptográfiai modulra" (MCSO-PP, HSM-PP),
- CEN 14167-3 munkacsoport egyezmény: „Védelmi profil hitelesítés-szolgáltató kulcs előállítási szolgáltatásait megvalósító kriptográfiai modulra" (CMCKG-PP, HSM-PP)
- CWA 14167-1, és a CWA 14172-1,-2,-3,-4 CEN Workshop Agreement-ek.

1.2. A HP azonosítása

A jelen szabályzat a **nyilvános körben kibocsátott minősített tanúsítványtípus [MTT]** kezelését, az ezzel kapcsolatos eljárásokat és szabályokat írja le.

Az **[MTT]** Biztonságos aláírás-létrehozó eszköz alkalmazását külön nem megkövetelő minősített tanúsítványtípus, amelyre vonatkozó követelmények a következők:

- megfelel az elektronikus aláírásról szóló 2001. évi XXXV. törvény 2. számú mellékletében meghatározott követelményeknek,

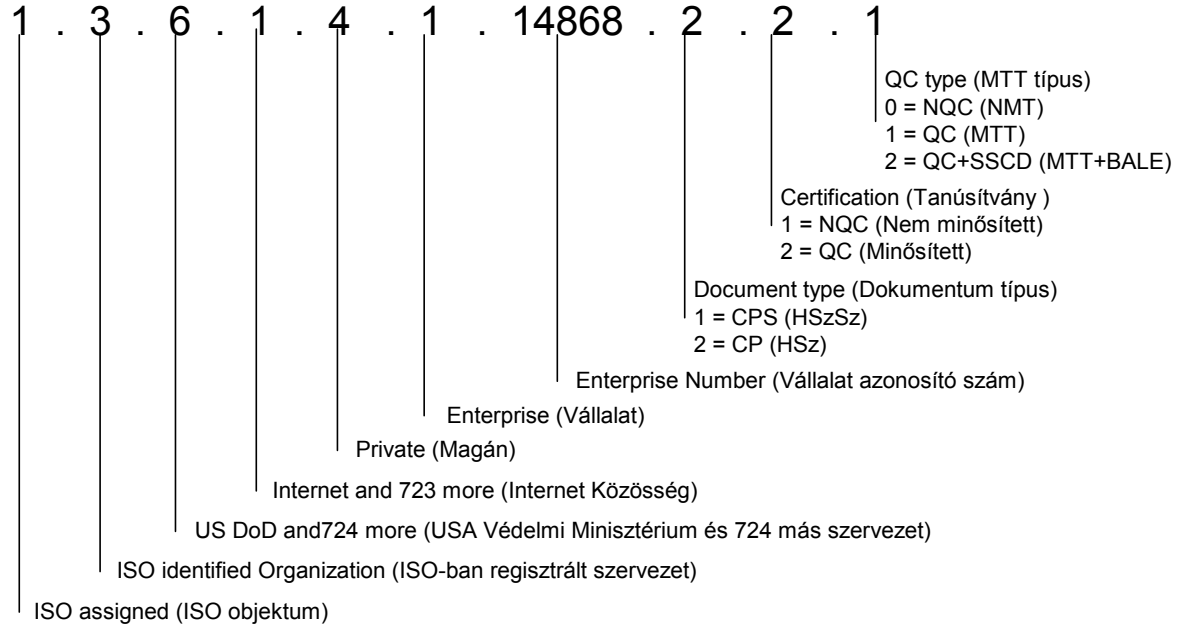
[2] ITSEC = Information Technology Security Evaluation Criteria (Információtechnológia Biztonsági Értékelési Kritériumok) az Európai Közösség ajánlása az IT termékek és rendszerek biztonságának funkcionális és minősítési követelményeire.

[3] CC = Common Criteria (Közös /Informatikai Biztonsági/ Követelmények) az Európai Közösség, az Egyesült Államok és Kanada közös ajánlása az IT termékek biztonsági minősítésének követelményeire.

- olyan Szolgáltató adta ki, amely teljesíti a 2001. évi XXXV. törvény 3. számú mellékletében meghatározott követelményeket,
- nyilvános körben került kibocsátásra.

Ezen alapkövetelmények alapján kibocsátott minősített tanúsítványok olyan elektronikus aláírások igazolására használhatók, amelyek jogérvényesíthetősége, jogi eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg[4].

A nyilvános körben kibocsátott minősített tanúsítványtípus objektum azonosítója:



Jelen dokumentum teljes neve: **A MÁV INFORMATIKA Kft. nyilvános körben kibocsátott minősített tanúsítványtípusra (MTT) érvényes Hitelesítési Politikája.** A jelen dokumentumban HP-ként történik rá hivatkozás. A HP a Szolgáltató belső dokumentuma.

Jelen HP-nek csak a Szolgáltató aláírásával ellátott változata tekinthető hitelesnek.

[4] Vagyis fokozott biztonságú, de nem minősített aláírásokhoz (lásd a 2001. évi XXXV. törvény 3.§. (8) bekezdését).

1.3. Hitelesítés szolgáltató és felhasználó közösség, alkalmazhatóság

A Szolgáltató által kibocsátott tanúsítványokat alkalmazó közösség a következő:

- a Szolgáltatóval kapcsolatban álló hitelesítő és regisztráló szervezetek,
- a Szolgáltató elektronikus aláírásra feljogosított munkatársai,
- a szerződéses előfizetők aláírói,
- a szerződéses előfizetők informatikai eszközei (szerverek, kommunikációs kapcsolatok, alkalmazások, stb.),
- az érintett felek.

1.3.1. Hitelesítési Politika és Szabályozási Csoport

A Hitelesítési Politika és Szabályozási Csoport a Szolgáltató által létrehozott szervezeti egység, amely a hitelesítés szolgáltatással kapcsolatos politikák és szabályzatok kialakításáért, elfogadásáért, karbantartásáért és adminisztrációjáért felelős.

A Hitelesítési Politika és Szabályozási Csoportnak függetlennek kell lennie a PKI Üzleti Egységtől. A Hitelesítési Politika és Szabályozási Csoport feladata általában a hitelesítés szolgáltatáshoz kapcsolódó politikák és szabályzatok elkészítése. Amennyiben a PKI Üzleti Egység vagy bármely más szervezeti egység, illetve külső megbízott készít el politikát vagy szabályzatot, akkor a Hitelesítési Politika és Szabályozási Csoportnak ellenőriznie kell azokat megfelelőség szempontjából.

1.3.2. Hitelesítő szervezet

A hitelesítő szervezet a Szolgáltató központi eleme, amely a szolgáltatás-támogató informatikai rendszer központi erőforrásaiból, azt ezt körül vevő biztonságos fizikai környezetből, valamint az üzemeltető és szolgáltatást ellátó személyzetből áll. Feladata a különböző osztályú és típusú aláírás létrehozó adatok és tanúsítványok előállítása, ezek nyilvános publikálása, a regisztráló szervezettől érkező módosítási, felfüggesztési, újra aktivizálási, visszavonási és megszüntetési igényeknek a Hitelesítés Szolgáltatási

Szabályzat (továbbiakban: HSzSz) szerinti végrehajtása és a szolgáltatás támogató informatikai rendszer üzemeltetése.

A Szolgáltatónál a hitelesítő szervezethez kapcsolódó feladat-, felelősség- és hatásköröket a PKI Üzleti Egység gyakorolja.

1.3.3. Regisztráló szervezet

A regisztráló szervezet és a vele szerződéses alapon együtt működő Társaságok (mint szerződött közreműködők) az előfizetők adatainak regisztrációját, ellenőrzését, az igénylő személyazonosságának és hitelességének megállapítását, a tanúsítvány kérelmek összeállítását, a regisztrációs szervezethez történő továbbítását végzik, és egyéb azonosítási, tanúsítványmenedzsment és adminisztrációs feladatokat látnak el.

Egy regisztráló szervezethez tartozó előfizetők önálló közösséget alkothatnak, melyre a Szolgáltató, vagy a vele szerződéses alapon együtt működő Társaságok (mint szerződött közreműködők) további szabályokat is alkalmazhatnak.
A regisztráló szervezet által létrehozott szabályok nem tartalmazhatnak olyan kikötést, amely ellentétben áll a Hitelesítési Politika és Szabályozási Csoport által jóváhagyott Szabályzatokkal.

A regisztráló szervezet az elektronikus aláírás hitelesítés-szolgáltatás keretein belül biztosítja az előfizetői regisztrációt, a tanúsítványok felfüggesztés és visszavonás kezelését és az Aláírás-létrehozó eszközön az Aláírás-létrehozó adat elhelyezését. Egyúttal közreműködik további elektronikus aláírással kapcsolatos szolgáltatások biztosításában: tanúsítvány előállítás, kibocsátás és visszavonási állapot közzététele.

A regisztráló szervezetek elérhetősége a „http://www.mavinformatika.hu/ca/" weboldalon található.

1.3.4. Végfelhasználók

1.3.4.1. Előfizető

Az Előfizető a Szolgáltatóval, az Általános Szolgáltatási Feltételekben foglaltak szerint szerződéses viszonyban álló felhasználó, aki számára a Szolgáltató a jelen HP-ben meghatározott típusú Tanúsítványt bocsát ki. Előfizető lehet természetes, illetve jogi személy.

Az Előfizető egyben Aláíró is, amennyiben saját maga képviseletében az aláírási jogosultsággal is rendelkezik, azaz birtokolja és használja az Aláírás létrehozó adatot.

Az Előfizető lehet jogi személy (szervezet) is. Ebben az esetben az Aláíró képviselőjeként egy természetes személyt bíz meg, akit felruház az aláírási jogosultsággal. Ez a személy a jogi személyt képviselve ír alá.

Tehát Aláíró lehet:

a) bármely magyar állampolgárságú természetes személy, aki személyazonosságát a regisztráció során az általa igényelt tanúsítvány osztálynak megfelelően, a HSzSz 3.1.8 pontjában előírtak szerint igazolta.

b) bármely természetes személy, aki részére a Tanúsítvány azzal a céllal kerül kibocsátásra, hogy az Aláírót más természetes vagy jogi személy (szervezet) képviseletében történő aláírásra jogosítsa fel. Ebben az esetben az Aláíró személyazonosságának ellenőrzése mellett a regisztráció során a HSzSz 3.1.8 pontjában meghatározott módon a képviseleti jogosultságot is ellenőrizni kell.

1.3.4.2. Érintett fél

Az Érintett fél olyan természetes vagy jogi személy, aki vagy amely az elektronikus dokumentum fogadója, és egy adott Tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el.

1.3.5. Alkalmazhatóság

1.3.5.1. Szabályzat hatálya

A HP időbeli hatálya

A HP időbeli hatálya a változáskezelési táblázatban feltüntetett jelen szabályzati verzióra érvényes hatálybalépés dátumától kezdődően határozatlan időre szól.

Időbeli hatálya megszűnik a szolgáltatási tevékenység beszüntetésekor, illetve egy újabb szabályzat verzió hatályba lépésékor.

A HP személyi hatálya

Az 1.3 pontban meghatározott hitelesítés szolgáltató és felhasználó közösségre terjed ki.

A HP tárgyi hatálya

A következőkre terjed ki:

- az 1. pontban meghatározott szolgáltatásokra,
- a Szolgáltatónak a hitelesítés szolgáltatással valamilyen kapcsolatban álló összes objektumaira, tárgyi eszközeire.

1.3.5.2. Szolgáltatás szintje

A Szolgáltató a 2001. évi XXXV. sz. elektronikus aláírásról szóló törvény szerinti fokozott biztonságú szolgáltatást nyújt a következő szolgáltatási termékek vonatkozásában:

- MTT Tanúsítvány létrehozási szolgáltatás
- Regisztráló szolgáltatás
- Egyedi-név szolgáltatás
- MTT Tanúsítvány szétosztási szolgáltatás
- Visszavonás kezelési szolgáltatás
- MTT Tanúsítvány archiválási szolgáltatás
- Állapotinformációs szolgáltatás
- Adattárolási szolgáltatás
- MTT Tanúsítvány megújítási szolgáltatás

A Szolgáltatónak a minősített hitelesítés szolgáltatást támogató eszközeit a nem minősített, illetve a teszt célú szolgáltatásokat támogató eszközeitől elválasztva kell használnia és üzemeltetnie.

A Szolgáltatás megfelelőségét a 2.7 pont alapján auditor vizsgálja és tanúsítja.

1.3.5.3. Tanúsítványok alkalmazhatósága

A jelen szabályzat érvényességi körében kibocsátott minősített tanúsítványok olyan elektronikus aláírások igazolására használhatók, amelyek jogérvényesíthetősége, jogi eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg[5].

A kibocsátott tanúsítványok (illetve az ezekhez kapcsolódó kulcspár) felhasználhatók minden olyan számítástechnikai alkalmazásban, amely támogatja a PKI technológián alapuló elektronikus aláírási, azonosítás-hitelesítési, le nem tagadhatósági funkciókat. A Tanúsítványhoz kapcsolódó magán- illetve publikus kulcsot kizárólag aláírás létrehozására, illetve ellenőrzésére lehet felhasználni a 2001. évi XXXV. sz. elektronikus aláírásról szóló törvény értelmében. A Szolgáltató nem vállal felelősséget az elektronikus aláírásra kibocsátott Tanúsítvány illetve az Aláírás létrehozó adat titkosításra, vagy más, az elektronikus aláírástól eltérő felhasználásáért.

Jelen HP hatálya alatt kibocsátott tanúsítványok csak az 1.3 fejezetben meghatározott Szolgáltató és felhasználó közösség körében használhatók Magyarországon az Általános Szerződési Feltételekben, illetve az Egyéni Szerződésben meghatározott összeghatárok szerinti korlátokkal.

A Tanúsítvány használati lehetőségére vonatkozó fenti információk a Tanúsítványban is rögzítésre kerülnek. A feltüntetett használati információktól bármely módon eltérő használat az Aláíró egyéni felelőssége és kockázata, ahogy az ilyen módon felhasznált Tanúsítvány elfogadása az aláírás ellenőrző felelőssége és kockázata.

1.4. Tanúsítvány osztály, tanúsítványtípus és tanúsítvány fajta

A Trust&Sign® tanúsítványok három bizalmi osztályba sorolhatók a létrehozott aláírás hitelességi szintje szerint:

- nem minősített (fokozott biztonságú szolgáltatás által létrehozott Tanúsítvány),
- minősített,
- teszt

[5] Lásd a 2001. évi XXXV. törvény 3.§. (8) bekezdését.

tanúsítványok osztálya.

A minősített tanúsítvány bizalmi osztályba két tanúsítványtípus tartozik:

- nyilvános körben kibocsátott minősített tanúsítványtípus (MTT),
- nyilvános körben kibocsátott Biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített tanúsítványtípus (MTT+BALE)

A jelen HP csak a nyilvános körben kibocsátott minősített tanúsítványtípusra (**MTT**) vonatkozik.

A felhasználás területe és célja szerint:

- előfizetői
- szolgáltatói

használati osztályokat különböztetünk meg.

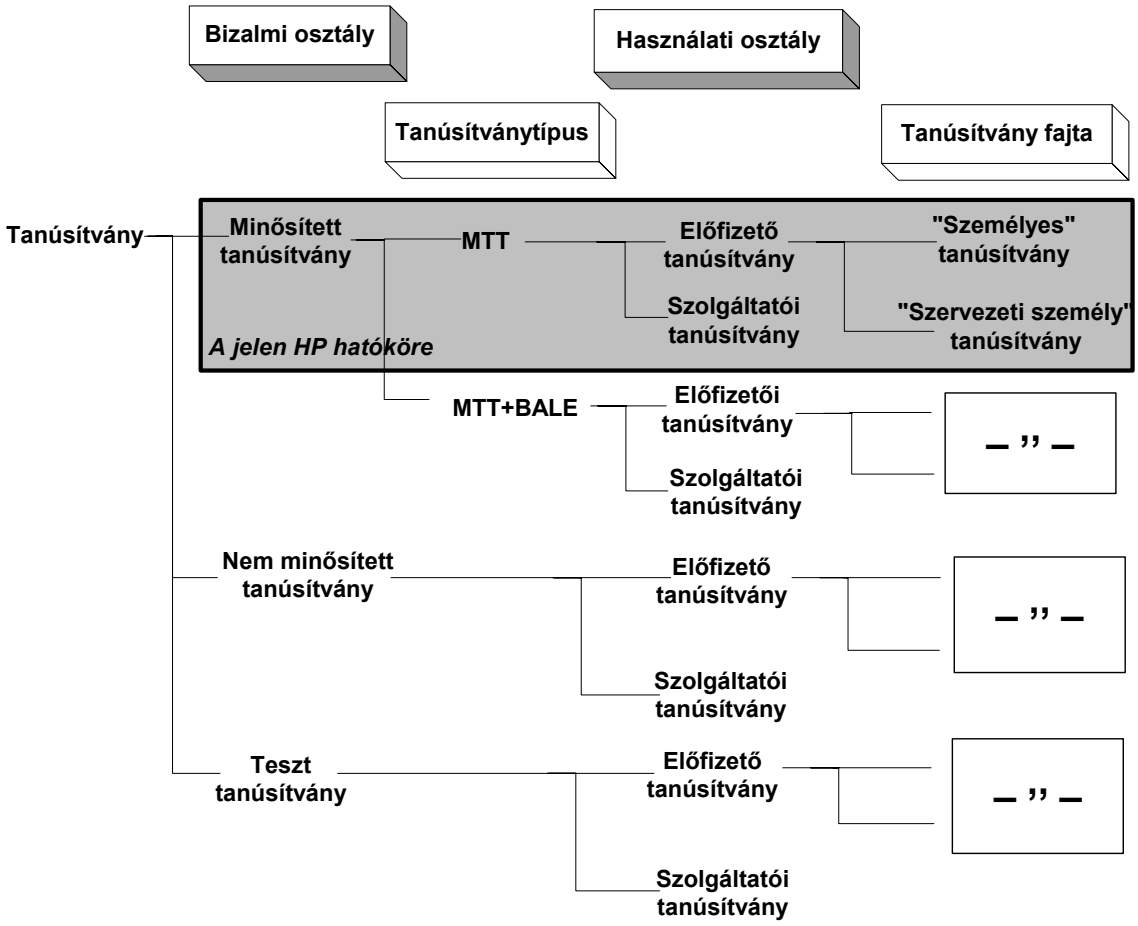
A Szolgáltató felelősségvállalása egyszintű, amelynek értéke a Trust&Sign® Tanúsítvány típusától függően, a felhasználó típusától és a felhasználási céltól függően kerül meghatározásra. A felelősségvállalás értékét az Előfizetői Szerződés rögzíti és ez az érték a Tanúsítványban is szerepel.

Felelősségvállalással Tanúsítvány értelemszerűen csak az Előfizetőnek adható ki. A felelősségvállalás mértékét az Előfizetői Szerződés rögzíti.

A jelen HP a következő tanúsítvány fajtákat különbözteti meg:

- „személyes" tanúsítvány,
- „szervezeti személy" tanúsítvány,

Az 1. ábra mutatja a tanúsítvány osztályok hierarchiáját. A szürke színnel jelzett terület foglalja magában a minősített tanúsítványok osztályába tartozó MTT és az MTT+BALE tanúsítványtípusokat.



1. ábra. Tanúsítvány osztályok, típusok és fajták

A minősített tanúsítvány osztály típusainak és fajtáinak jellemzőit az 1.4.2 és 1.4.3 pontok írják le.

1.4.1. A minősített tanúsítvány osztály jellemzői és típusai

1.4.1.1. A minősített tanúsítvány jellemzői

Minősített tanúsítvány az elektronikus aláírásról szóló 2001. évi XXXV. törvény 2. számú mellékletében foglalt követelményeknek megfelelő olyan Tanúsítvány, melyet minősített szolgáltató bocsátott ki.

A 2001. évi XXXV. törvény 2. számú melléklete szerint a minősített tanúsítványoknak tartalmazniuk kell az alábbiakat:

1. annak megjelölését, hogy a Tanúsítvány minősített tanúsítvány,

2. a Szolgáltató és székhelyének (ország-) azonosítóját,
3. az Aláíró nevét vagy egy álnevet[6], ennek jelzésével,
4. az Aláírónak külön jogszabályban, illetve a szolgáltatási szabályzatban, illetőleg az ÁSzF-ben meghatározott speciális jellemzőit, a Tanúsítvány szándékolt felhasználásától függően,
5. azt az Aláírás-ellenőrző adatot, amely az Aláíró által birtokolt aláírást készítő adatnak felel meg,
6. a Tanúsítvány érvényességi idejének kezdetét és végét,
7. a Tanúsítvány azonosító kódját,
8. az adott minősített tanúsítványt kibocsátó Szolgáltató fokozott biztonságú elektronikus aláírását,
9. a Tanúsítvány használhatósági körére vonatkozó esetleges korlátozásokat,
10. a Tanúsítvány felhasználásának korlátjait,
11. más személy (szervezet) képviseletére jogosító elektronikus aláírás Tanúsítványa esetén a Tanúsítvány ezen minőségét és a képviselt személy (szervezet) adatait.

A jelen szabályzat a nyilvános körben kibocsátott minősített tanúsítványtípusra (**MTT**) vonatkozó hitelesítési szabályokat határozza meg.

Az **MTT** olyan tanúsítványtípus, amely:

- ♦ megfelel a 2001. évi XXXV. törvény 2. számú mellékletében meghatározott követelményeknek,
- ♦ olyan Szolgáltató adta ki, amely teljesíti a 2001. évi XXXV. törvény 3. számú mellékletében meghatározott követelményeket,
- ♦ nyilvános körben került kibocsátásra.

1.4.2. Minősített tanúsítványok használati osztályainak jellemzői

1.4.2.1. Előfizetői Tanúsítvány

Előfizetői Tanúsítvány a Szolgáltatóval az Előfizetői Szerződés által szerződéses viszonyba kerülő Előfizető számára kibocsátott Tanúsítvány.

[6] A Szolgáltató a tanúsítványban álnév feltüntetését vállalja.

Előfizetői Tanúsítvány csak felelősség vállalással bocsátható ki, amelynek értékét az ÁSzF vagy ettől eltérő értékben történő megállapodás esetén az Előfizetővel történt megállapodás határozza meg.

Előfizetői Tanúsítvány olyan természetes személyeknek vagy szervezeteknek kerül kiadásra, amelynél az Aláírót személyes megjelenésre, saját hitelesítő dokumentumokra és írásos nyilatkozatokra alapozott biztonsági ellenőrzéssel kell a Szolgáltatónak azonosítani és hitelesíteni.

Az azonosítás-hitelesítés módját a 1. táblázat határozza meg.

Azonosítás-hitelesítés alanya	Azonosítás-hitelesítés módja
Természetes személy	Személyi igazolvány vagy útlevél bemutatása személyesen
Szervezeti személy	Személyi igazolvány vagy útlevél bemutatása személyesen, képviseleti megbízás cégszerűen aláírva, 30 napnál nem régebbi cégkivonat, aláírási címpéldány

1. táblázat

Amennyiben a természetes személy bármely más természetes vagy jogi személyt képvisel, akkor a képviseleti jogot írásos megbízói nyilatkozattal kell igazolni. Amennyiben a természetes személy jogi személyt képvisel, akkor a szervezetnek írásban kell nyilatkoznia arról is, hogy az Aláíró hiteles személyazonosságának megállapítása a szervezeten belül már előzetesen megtörtént.

A Szolgáltató a megbízott képviselő személyt nyilvántartja és bármely, a képviselt személy nevében történő eljárás esetén a képviselő személy azonosítását-hitelesítését az Aláíró, illetve az Előfizető esetében szokásos eljárásnak megfelelően el kell végezni.

1.4.2.2. Szolgáltatói Tanúsítvány

A szolgáltatói tanúsítványokat Szolgáltató csak saját célra bocsátja ki, a szolgáltatási termékek előállításának biztosítására. Előfizető ezeket nem igényelheti.

1.4.3. Tanúsítvány fajták és tulajdonságaik

A következőkben meghatározott fajtájú, minősített tanúsítványok kiadhatók előfizetők részére, illetve a Szolgáltató saját céljaira.

1.4.3.1. „Személyes” tanúsítvány

Személyes tanúsítványokat magyar állampolgárságú természetes személy igényelhet a saját nevében.
Az Előfizető és az Aláíró ugyanaz a személy.

A regisztráló szervezetnél történő azonosítás-hitelesítésnél a következő adatokat kell kezelni:

- az Aláíró neve, aláírása,
- az Aláíró okmányszáma (személyi igazolvány vagy útlevél szám),
- az Aláíró lakcíme,
- az Aláíró e-mail címe.

A Tanúsítvány „Country” és „Locality” mezőjében az Aláíró lakóhelyének országkódja és helyiségneve, az „Organization” és „Organization Unit” mezőkben semmi, a „Common Name” mezőben az Aláíró neve, az „E” mezőben az Aláíró e-mail címe, szerepel. Amennyiben az Aláíró hozzájárul a Tanúsítvány „STREET” mezőjében az Aláíró lakcímében szereplő utca neve és a házszám, a „PostalCode” mezőjében az Aláíró lakcímében szereplő irányítószám is szerepel.

1.4.3.2. „Szervezeti személy” tanúsítvány

Meghatalmazásos tanúsítványokat természetes személy igényelhet egy adott szervezet alkalmazottjaként és/vagy tisztségviselőként. A szervezet - többek között - lehet gazdálkodó szervezet, hivatal, önkormányzat, egyesület, alapítvány.

Ebben az esetben az Előfizetőnek a képviselt szervezet, Aláírónak a szervezetet képviselő személy számít. Az Előfizetői Szerződésben a szervezet által vállalt kötelezettségek egyetemlegesen érvényesek arra az Aláíróra, aki számára a szervezet a Tanúsítványt igényelte.

A regisztráló szervezetnél történő azonosítás-hitelesítésnél a következő adatokat kell kezelni:

- az igénylő szervezet neve, székhelye,
- annak a szervezeti egységnek a neve, e-mail címe, telefon+fax száma, amely az aláírásra kijelölt személyt megbízza,
- a képviseleti megbízás dokumentuma cégszerűen aláírva,
- az aláírásra kijelölt személy neve, aláírása,
- annak a szervezeti egységnek a megnevezése, ahol az aláírásra kijelölt személy dolgozik,

- az aláírásra kijelölt személy beosztása,
- az aláírásra kijelölt személy személyi igazolvány vagy útlevél száma,
- az aláírásra kijelölt személy telefon száma, e-mail címe.

A fentieken kívül még a következőket kell megadni:

- az aláírásra kijelölt személy kijelölését engedélyező személy neve, aláírása; az engedélyezőnek minden esetben cégképviseletre jogosult személynek kell lennie és ezt aláírási címpéldánnyal kell igazolni,
- az engedélyező beosztása,
- az engedélyező személy munkahelyi telefonszáma, fax-száma, e-mail címe.
- az igénylő szervezet nevében a későbbiekben eljáró képviselő személy neve, aláírása, beosztása személyi igazolvány vagy útlevél száma, hivatali telefonszám és e-mail címe,
- az igénylő szervezet által hitelesített megbízó levél, amelyben az a képviselő személyt az igénylő szervezet nevében történő eljárásra megbízza.

A Tanúsítvány „Country" és „Locality" mezőjében az igénylő szervezet székhelyének vagy telephelyének országkódja és városa, az „Organization" mezőben az igénylő szervezet neve, az „Organizational Unit" mezőben az igényt támasztó szervezeti egység neve, a „Common Name" mezőjen az aláírásra kijelölt szervezeti személy neve, a „STREET" mezőben az az igénylő szervezet székhelyének vagy telephelyének címében szereplő utcanév és a házszám, a „PostalCode" mezőben a címben szereplő irányítószám, az „E" mezőben az aláírásra kijelölt szervezeti személy e-mail címe szerepel.

A Tanúsítvány egyéb ellenőrzött adatokat is tartalmazhat, különböző kiterjesztés mezőkben.

1.5. Szolgáltató adatai

1.5.1. Cím, cégjegyzékszám, kontakt információk

Név: MÁV Informatika Kereskedelmi, Szolgáltató és Tanácsadó Korlátolt Felelősségű Társaság

Cégjegyzék szám: 01-09-563711

Székhely, telephely: 1012 Budapest, Krisztina krt. 37/a.

Telefonszám: (36-1) 457-9322

Telefax szám: (36-1) 457-9520

Internet cím: http://www.mavinformatika.hu

Panaszok bejelentésének helye:

- írásban a Szolgáltató telephelyére címezve
- telefonon és faxon az ügyfélszolgálatnál
- elektronikus levélben a Help Desk e-mail címére,

Illetékes fogyasztóvédelmi felügyelőség:

Budapest Főváros Közigazgatási Hivatal Fogyasztóvédelmi Felügyelőség,
1088 Budapest, József krt. 6.,
Levélcím: 1364. Budapest, Pf. 234.,
telefon: 4594-918, telefax: 4594-870

A HIF által minősített szolgáltatóként történő nyilvántartásba vétel napja:

……..

A HIF által minősített szolgáltatóként történő nyilvántartás (regisztráció) száma:

……...

1.5.2. Ügyfélszolgálat

A vevői kapcsolatok biztosítása érdekében a Szolgáltató ügyfélszolgálatot tart fenn, amelyet a regisztráló szervezet és a Help Desk támogat.
Az Ügyfélkapcsolati Iroda címe: Budapest, I. Krisztina krt. 37/a.
Az Ügyfélkapcsolati Iroda munkanapokon 9 és 13 óra között áll az ügyfelek rendelkezésére, a Help Desk 24 órás szolgálatot ad.
Az Ügyfélkapcsolati Iroda elérhető telefonon a +36-1-457-93-93 előfizetői számon vagy a 06-80-39-93 93 zöld számon.
A Help Desk elérhető az ügyfélkapcsolati iroda telefonszámain, vagy elektronikus levélben a: **helpdesk@mavinformatika.hu** címen.
Szolgáltató regisztráló szervezeténél és Help Desk-jénél ügyfélszolgálati naplót kell vezetni, amelyben minden megkeresésről a következő információkat kell rögzíteni:

- A megkereső személy vagy szervezet neve,
- A megkeresés dátuma, időpontja,

- A megkeresés témájának rövid leírása,
- A felvetett kérdés, probléma elintézése, dátummal, időponttal.

1.5.3. Hitelesítési Politika és Szabályozási Csoport adatai

A Trust&Sign Hitelesítés Politika és Szabályozási Csoport elérhető a 1012 Budapest, I. Krisztina krt. 37/a címen, illetve telefonon a +36-1-457-93-00 központi számon.

2. Általános rendelkezések

2.1. Feladatok és hatáskörök

2.1.1. A MÁV INFORMATIKA Kft. feladatai és hatásköre

A MÁV INFORMATIKA Kft., mint Szolgáltató kötelezettséget vállal arra, hogy az Szervezeti és Működési Szabályzatban, a mindenkori HSzSz-ben és HP-ben, az Általános Szolgáltatási Feltételekben és az Előfizetői Szerződésekben és a Biztonsági Szabályzatban meghatározottak szerint jár el az előfizetők tanúsítványainak kiadásakor és kezeléskor, amelynek keretében kötelezettséget vállal az alábbiakra:

1. A Szolgáltató (a hitelesítő szervezet, a regisztráló szervezet, és a Címtár együttes tevékenységével) az alábbi, elektronikus aláírással kapcsolatos szolgáltatásokat biztosítja:

   elektronikus aláírás hitelesítés-szolgáltatás (a továbbiakban: hitelesítés-szolgáltatás), ezen belül:

   - regisztráció,
   - tanúsítvány előállítás,
   - kibocsátás,
   - visszavonás kezelés,
   - visszavonási állapot közzététele

2. A Szolgáltató gondoskodik a Szolgáltatóra és a szolgáltatásra vonatkozó valamennyi, a jelen HP és a HSzSz 3.-8. pontjaiban részletezett állítás teljesüléséről, amennyiben azok az adott tanúsítványtípusra alkalmazhatóak.
3. A Szolgáltató szolgáltatásait hozzáférhetővé teszi minden olyan igénylő számára, akinek tevékenysége kinyilvánított működési területére esik.
4. A Szolgáltató jogi személy.
5. A Szolgáltató megfelelően dokumentált megállapodásokkal és szerződéses kapcsolatokkal rendelkezik azon esetekre, amikor a szolgáltatások nyújtása alvállalkozókat, illetve más, harmadik felekkel kötött megegyezéseket érint.

6. A Szolgáltató olyan HSzSz-el rendelkezik, mely a tanúsítványtípusban azonosított valamennyi követelmény kielégítésére szolgáló gyakorlatra és eljárásra vonatkozik.
7. A Szolgáltató a HSzSz-ben meghatározza a szolgáltatásait támogató valamennyi külső szervezetre vonatkozó kötelezettségeket, beleértve az alkalmazandó szabályzatokat és gyakorlatokat is.
8. A Szolgáltató valamennyi szolgáltatását a HSzSz-el összhangban nyújtja.
9. A HSzSz-t a Szolgáltató felsőszintű irányító testülete hagyja jóvá.
10. A HSzSz megfelelő megvalósításáért a Szolgáltató felső vezetősége felel.
11. A Szolgáltató rendszeresen felülvizsgálja HSzSz-ét, az újra érvényesített szabályzat tartalmazza a szükséges módosításokat.
12. A Szolgáltató időben értesítést tesz közzé a szolgáltatási szabályzatában tervezett változtatásokról és a fenti (a 9. pont szerint történő) jóváhagyást követően az átdolgozott szolgáltatási szabályzatát (a 19. pontban előírtak szerint) haladéktalanul hozzáférhetővé teszi.
13. A Szolgáltató mindenkor az Aláíró által szolgáltatott, az Ügyfélkapcsolati Iroda által a HSzSz-ben és Előfizetői Szerződésben meghatározott módon jóváhagyott adatok alapján bocsátja ki a Tanúsítványt.
14. A Szolgáltató a Tanúsítvány kibocsátását követően a Tanúsítvány adataiban változást nem eszközölhet. Az Előfizető, illetve Aláíró által – a Tanúsítványban foglalt adatok változására vonatkozó – bejelentés automatikusan a Tanúsítvány visszavonását vonja maga után. A módosított adatokkal kibocsátott Tanúsítvány új Tanúsítványnak minősül.
15. Amennyiben a Szolgáltató észlelése vagy megállapítása szerint az adatok nem felelnek meg a valóságnak köteles ezt jelezni az Előfizető részére és kérni az adatok helyesbítését. Amennyiben a felhívásban megjelölt határidőig a helyesbítés elmarad, a Szolgáltató megtagadja a Tanúsítvány kiadását.
16. A Szolgáltató kötelezettséget vállal arra, hogy a tanúsítványigénylésnek a HP-ben rögzítetteknek megfelelően történő elbírálását követően a HSzSz 2.1.1/13 pontjában meghatározott módon és időn belül a Tanúsítványigénylés feldolgozásáról intézkedik. Jogi személy képviseletére jogosító Tanúsítvány esetén a képviselt szervezetet a regisztráló szervezet értesíti. A Szolgáltató e mellett nyilvántartást vezet a Tanúsítvány kérelmek státusának állásáról, amelyet a HSzSz 2.6 pontjában meghatározott módon tesz hozzáférhetővé a regisztráló szervezet részére.

17. A Szolgáltató a szolgáltatás üzemeltetése során a HSzSz-ben, az ÁSzF-ben illetve az Előfizetői Szerződésben rögzített ügyfélszolgálati tevékenységet a regisztráló szervezet által biztosítja, amely egy műszakban fogadja az igénylőket, megadja a szükséges tájékoztatást és információkat, szerződést köt, átadja az Aláírás létrehozó eszközöket, fogadja a tanúsítvány visszavonási igényeket.
18. A Szolgáltató a Help Desk szolgáltatása keretében folyamatos 24 órás felügyeletet biztosít az előfizetői kérdések, panaszok, felfüggesztési és visszavonási igények kezelésére.
19. A Szolgáltató vezeti és közzéteszi a jogszabály szerinti nyilvántartásokat, valamint a Tanúsítvány kibocsátására vonatkozó saját szabályzatait (HSzSz, Általános Szolgáltatási Feltételek /a továbbiakban: ÁSzF/), Internet segítségével, bárki számára folyamatosan elérhető módon. Ezen szabályzatok elérési helye a http://www.mavinformatika.hu/ca/ web oldal.
20. A Szolgáltató értesítést küld a lejáró Tanúsítványokról az Előfizető és az Aláíró részére a HSzSz 2.1.1/16 pontjában meghatározott módon és időn belül a lejárat előtt. Felhívja az Előfizető és az Aláíró figyelmét arra, hogy a Tanúsítvány lejáratát követően azt nem használhatja. Amennyiben az Előfizető, illetve az Aláíró a Tanúsítvány lejártáig nem rendelkezik a Szolgáltató felé, az esetben a Tanúsítvány lejár, és a Szolgáltató adott Tanúsítványra vonatkozó szolgáltatási kötelezettsége a HSzSz-ben vállalt további adattárolási kötelezettségek kivételével megszűnik.
21. Szolgáltató köteles a Tanúsítvány megfelelő mezőjében feltüntetni, ha az ÁSzF, illetve az Előfizetői Szerződés a Tanúsítvány felhasználhatóságával kapcsolatban összeg, területi vagy egyéb korlátozásokat köt ki.
22. A Szolgáltató felfüggeszti a Tanúsítvány érvényességét és ezt a HSzSz-ben meghatározott helyen közzéteszi, ha
    22.1. az Előfizető vagy az Aláíró ezt az ÁSzF-ben meghatározott módon kéri,
    22.2. a szolgáltatással kapcsolatos – jogszabályban meghatározott – rendellenességről szerez tudomást,
    22.3. megalapozottan feltételezhető, hogy a Tanúsítványban foglalt adatok nem felelnek meg a valóságnak, vagy az Aláírás létrehozó adat nem az Aláíró kizárólagos birtokában van,
    22.4. A Hírközlési Felügyelet jogerős és végrehajtható határozatában így rendelkezik.

A felfüggesztés kezdeményezésének módjáról, a felfüggesztett státusz fenntartásának maximális időtartamáról, valamint a felfüggesztés feloldásáról, az aktív státusz visszaállításának indokairól és körülményeiről minden esetben a HSzSz-nek kell rendelkeznie.

23. A Szolgáltató köteles a Tanúsítvány visszavonására és ennek közzétételére az alábbi esetekben:
    23.1. amennyiben ezt az Aláíró, szervezeti személy típusú Tanúsítvány esetén az általa képviselt jogi személy a mindenkori HSzSz-ben, illetve az ÁSzF-ben meghatározott módon kéri,
    23.2. amennyiben a képviseleti jogosultság megszűnéséről a képviselt természetes vagy jogi személy, a képviselője, illetve az Aláíró a Szolgáltatónak bejelentést tesz,
    23.3. amennyiben a Szolgáltató a szolgáltatással kapcsolatos – jogszabályban, vagy a HSzSz-ben meghatározott – rendellenességről vesz tudomást és a rendellenesség az ezen dokumentumokban meghatározott szabályok szerint nem orvosolható,
    23.4. amennyiben tudomására jut, hogy a Tanúsítványban foglalt adatok nem felelnek meg a valóságnak, vagy az Aláírás létrehozó adat nem az Aláíró kizárólagos birtokában van,
    23.5. a Szolgáltató és az Előfizető között a szerződés megszűnt,
    23.6. a HIF jogerős és végrehajtható határozatában így rendelkezik,
    23.7. a Szolgáltató a tevékenységét befejezte.
24. A Szolgáltató kötelezettséget vállal arra, hogy a részére beadott visszavonási kérelmeket a HP-ben, valamint az ÁSzF-ben meghatározott feltételek szerint feldolgozza, és a visszavont Tanúsítványok a visszavonási listákon közzétételre kerülnek.
25. A Tanúsítványok lejárat előtti visszavonásának jogkövetkezményei az alábbiak:
    25.1. a visszavont Tanúsítvány a továbbiakban a jelen HP 1.3.5.3 pontjában meghatározott tevékenységek végzésére nem használható. Ha az Aláíró az Aláírás létrehozó adatot felhasználja, az aláírás ellenőrzője jogosult az elfogadás megtagadására,
    25.2. a visszavonást követően nem kerül automatikusan új Tanúsítvány kibocsátásra; azt az új Tanúsítványok igénylésével azonos igénylési folyamatnak kell megelőznie.

26. Szolgáltató megőrzi a Tanúsítványokkal kapcsolatos elektronikus információkat és az ahhoz kapcsolódó személyes adatokat legalább a Tanúsítvány érvényességének lejáratától számított öt évig, illetőleg – amennyiben ezen időszakban az elektronikus aláírással, illetve az azzal aláírt elektronikus dokumentummal kapcsolatosan jogvita merül fel és azt a Szolgáltatónak írásban bejelentették – a jogvita jogerős lezárásáig. Ugyanezen határidőig olyan eszközt is biztosít, mellyel a kibocsátott Tanúsítvány tartalma megállapítható.
27. A Szolgáltató tevékenységi köréből csak az új Tanúsítvány kibocsátást szüneteltetheti. A Szolgáltató köteles szüneteltetni tevékenységét, ha a Hírközlési Felügyelet az elektronikus aláírásról szóló 2001. évi XXXV. törvény 21. § (1) bekezdés c) pontja alapján ideiglenes intézkedésként elrendeli az új Tanúsítvány kibocsátási tevékenység szünetelését és ezt a tényt feltünteti a nyilvántartásban.
28. Ha a Szolgáltató be kívánja fejezni tevékenységét, erről a tevékenység befejezését a HSzSz 2.1.1/29 pontjában meghatározott időpontot megelőzően értesítenie kell az előfizetőket, az általa kibocsátott és még vissza nem vont Tanúsítványok Aláíróit, általuk képviselt természetes vagy jogi személyt, valamint a Hírközlési Felügyeletet, megjelölve a 29. bekezdés szerinti szervezetet. A bejelentés időpontjától kezdve a Szolgáltató nem bocsáthat ki új Tanúsítványt. A Szolgáltató a tevékenység befejezését legalább húsz napot megelőzően köteles az általa kibocsátott, és még vissza nem vont Tanúsítványokat visszavonni. A Szolgáltató Tanúsítványok visszavonását követően a tevékenysége befejezéséig a nyilvánosságra hozatali kötelezettségének továbbra is köteles eleget kell tenni.
29. A Szolgáltató intézkedik az iránt, hogy legkésőbb a tevékenység befejezésekor más - vele legalább azonos besorolású - szolgáltató átvegye nyilvántartásait, így különösen a visszavont Tanúsítványok nyilvántartását, valamint ellássa a hatályos jogszabályokban foglalt feladatokat. A Szolgáltató a visszavont Tanúsítványokkal kapcsolatos minden adatot - beleértve a személyes adatokat is – átadja ezen szolgáltatónak, amely kötelezettséget vállal azoknak az 1995. évi CXXII. tv. a polgárok személyes adatainak nyilvántartásáról szóló 1992. évi LXVI. tv. módosítása szerinti kezelésére.
30.

2.1.2. A hitelesítő szervezet feladatai és hatásköre

A Szolgáltató által működtetett hitelesítő szervezetek feladata és hatásköre általában az elektronikus aláírással kapcsolatos alábbi szolgáltatás megvalósítása:

- tanúsítvány előállítás;

  egyúttal közreműködik (a visszavonási listák aláírásával) a visszavonási állapot közzétételében.

A hitelesítő szervezetek a tanúsítvány előállítás szolgáltatás biztosítása keretén belül:

1. ellenőrzik a regisztráló szervezettől érkező tanúsítvány kérelmet, benne az aláírandó tanúsítvány adatokat tartalmazó üzenet sértetlenségét és hitelességét,
2. feldolgozzák a regisztráló szervezettől érkező hiteles és sértetlen tanúsítvány kérelmet, melynek keretén belül előállítja a Tanúsítványt (aláírja az aláírandó tanúsítvány adatokat),
3. csak tanúsítványok aláírására használják fel a Tanúsítvány aláírására használt magánkulcsukat,
4. csak olyan tanúsítványokat állítanak elő, amelyek megfelelnek a HSzSz-ben meghatározott, támogatott tanúsítványtípusoknak,
5. gondoskodnak arról, hogy a Tanúsítványban foglalt megkülönböztetett név egyedi legyen a Szolgáltató szolgáltatási körén belül,
6. gondoskodnak arról, hogy a Szolgáltató teljes szolgáltatási körén belül kibocsátott tanúsítványokhoz tartozó kulcsok mindvégig egyediek maradjanak,
7. megválaszolják a regisztráló szervezetnek a tőle kapott tanúsítvány kérelmet, benne elküldve az előállított Tanúsítványt, biztosítva a válaszüzenet sértetlenségét és hitelességét.

A hitelesítő szervezetek a visszavonási állapot közzététele szolgáltatásban való közreműködés keretén belül:

1. ellenőrzik a regisztráló szervezettől érkező visszavonási lista aláírási kérelmet, s ebben az aláírandó Tanúsítvány visszavonási lista sértetlenségét és hitelességét,
2. feldolgozzák a regisztráló szervezettől érkező hiteles és sértetlen visszavonási lista aláírási kérelmet, melynek során aláírja a Tanúsítvány visszavonási listát,
3. rendszeresen új Tanúsítvány visszavonási listát készítenek a tanúsítvány állapot adatbázisból, naponta egyszer, a szolgáltatási szabályzatban meghatározott frissítési időponthoz igazodóan, mely tartalmazza a következő lista tervezett kibocsátási idejét is,

4. csak tanúsítvány visszavonási listák aláírására használják fel a tanúsítvány visszavonási listák aláírására használt magánkulcsát,
5. megválaszolják a regisztráló szervezettől kapott visszavonási lista aláírási kérelmet, elküldve az aláírt Tanúsítvány visszavonási listát, biztosítva a válaszüzenet sértetlenségét és hitelességét.

Az Elsődleges (Root) hitelesítő szervezet alapvető feladata és hatásköre a produktívhitelesítő szervezet(ek), és a Szolgáltató döntése alapján további hitelesítő központok hitelesítése, ezen belül a feladatok tételesen a következők:

1. Saját kulcs-pár generálása.
2. A saját magánkulcsának MeH 12. ajánlás szerinti fokozott biztonságú védelme.
3. Saját Tanúsítvány előállítása önhitelesítéssel.
4. Saját Tanúsítvány nyilvánosságra hozatala.
5. Produktív hitelesítő szervezetek, hitelesítési kérelmeinek fogadása és ellenőrzése.
6. Kulcs-pár generálás és Tanúsítvány előállítás Szolgáltató hitelesítő szervezetek részére.
7. Produktív hitelesítő szervezetek Tanúsítvány visszavonási kérelmeinek feldolgozása.
8. Produktív hitelesítő szervezetek Tanúsítvány megújítási kérelmeinek feldolgozása.
9. Magánkulcs és Tanúsítvány a produktív hitelesítő szervezetekhez történő eljuttatása.
10. Produktív hitelesítő szervezetek Tanúsítványainak és visszavonási listáinak publikálása a Címtárban.
11. Produktív hitelesítő szervezet Tanúsítványának visszavonása, illetve felfüggesztése, amennyiben magánkulcsa kompromittálódik, vagy ennek gyanúja áll fenn.
12. Az általa tanúsított hitelesítő szervezetek bizalmi és biztonsági ellenőrzése.

A Produktív hitelesítő szervezet alapvető feladat és hatásköre a regisztráló szervezet által ellenőrzött és regisztrált előfizetők hitelesítése, ezen belül a feladatok tételesen a következők:

1. A saját Magánkulcsának MeH 12. ajánlás szerinti fokozott biztonságú védelme.
2. A regisztráló szervezet hitelesítési kérelmeinek fogadása és ellenőrzése.
3. A regisztráló szervezet tájékoztatása a tanúsítványkérelmek státuszáról.
4. Kulcs-pár generálás és Tanúsítvány előállítás a regisztráló szervezet részére.
5. Kulcs-pár és Tanúsítvány eljuttatása a regisztráló szervezethez.
6. A regisztráló szervezettől az előfizetői hitelesítési kérelmek fogadása és ellenőrzése.
7. Tanúsítvány előállítás az előfizetők részére.

8. A regisztráló szervezettől érkező tanúsítvány visszavonási, felfüggesztési és újraérvényesítési kérelmek feldolgozása.
9. A regisztráló szervezettől érkező tanúsítvány megújítási kérelmek feldolgozása.
10. Tanúsítványok és tanúsítvány visszavonási listák publikálása a Címtárban.
11. Intézkedni tanúsítványok visszavonása, illetve felfüggesztése végett, amennyiben magánkulcsa kompromittálódik, vagy ennek gyanúja áll fenn.
12. 99.9%-os rendelkezésre állás biztosítása a tanúsítvány felfüggesztési és visszavonási kérelmek végrehajtása érdekében.
13. A regisztráló szervezetek bizalmi és biztonsági ellenőrzése.

2.1.3. A Hitelesítési Politika és Szabályozási Csoport feladatai és hatásköre

A Hitelesítési Politika és Szabályozási Csoport a PKI Üzleti Egységtől függetlenül működik. Kötelessége a Szolgáltató és felhasználó Közösség igényeinek felmérése és folyamatos követése, ezek alapján a közösség működésére vonatkozó alapelvek, politikák lefektetése, s ebből levezetve a tagok tevékenységét részletesen szabályozó, az egész Szolgáltató szervezetre nézve közös szabályzatok, így a HP, a HSzSz, az ÁSzF, az Előfizetői Szerződések és a Biztonsági Szabályzat, készítése és rendszeres karbantartása változatkövetéssel.

A Hitelesítési Politika és Szabályozási Csoport feladatai tételesen a következők:

1. A Szolgáltató és felhasználó Közösség igényeinek felmérése.
2. A HP-k elkészítése és karbantartása.
3. A HP-k, a HSzSz, az ÁSzF, az Előfizetői Szerződések és a Biztonsági Szabályzat elkészítése és karbantartása.
4. A HP-k és a HSzSz közötti összhang rendszeres ellenőrzése és karbantartása.
5. A hitelesítés szolgáltatás támogató informatikai rendszer PKI alkalmazás szintű biztonsági ellenőrzése.
6. Szolgáltatók belső folyamatainak, tevékenységének szabályozása a közös szabályzataikon keresztül.
7. A szolgáltatók és a felhasználók közötti folyamatok szabályozása.
8. A szabályzatok karbantartása és változáskezelése.
9. A szolgáltatói szabályzatok verzióinak nyilvántartása és megőrzése.

10. A Szolgáltató és felhasználó Közösség tájékoztatása.
11. Nyilvános szabályzatok publikálása.
12. A regisztrációs folyamat szabályozása, ellenőrzése, felülvizsgálata.

2.1.4. A regisztráló szervezet feladatai és hatásköre

A regisztráló szervezet biztosítja az alábbi elektronikus aláírással kapcsolatos szolgáltatásokat:

- elektronikus aláírás hitelesítés-szolgáltatás (a továbbiakban: hitelesítés-szolgáltatás), ezen belül:
  - regisztráció,
  - visszavonás kezelés,
- Aláírás-létrehozó eszközön az Aláírás-létrehozó adat elhelyezése.

A regisztráló szervezet egyúttal közreműködik az alábbi elektronikus aláírással kapcsolatos szolgáltatások biztosításában:

- tanúsítvány előállítás,
- kibocsátás
- visszavonási állapot közzététele

A regisztráló szervezet az aláírók, az előfizetők és az érintett felek részére nyújtott regisztráló szolgáltatásán belül:

1. gondoskodik az Aláíró megfelelő azonosításáról, illetve arról, hogy a tanúsítványt igénylő formanyomtatványok teljesek, pontosak és kellőképpen hitelesek legyenek,
2. ellenőrzi az HSzSz 3.1 pontjában és az ÁSzF-ben előírt adatszolgáltatási követelmények szerint megadott adatok alapján a Tanúsítványt igénylő ügyfél (természetes, illetve szervezeti) személyazonosságát és a leendő Aláíró azon egyedi jellemzőit, melyet a minősített tanúsítvány igazol,
3. összegyűjti, illetve meghatározza a regisztráció során valamennyi, a HSzSz 3.1 pontjában meghatározott, Tanúsítványba kerülő adatot, ellenőrzi az Igénylő által átadott dokumentumok valódiságát, érvényességét, sértetlenségét és hitelességét,
4. összeveti egymással és a valósággal az egyes iratokon szereplő adatokat (így különösen a Tanúsítványt személyesen igénylő ügyfél fotóját az arcával, aláírását a helyszíni aláírásával),

5. ellenőrzi a dokumentumok érvényességét, valódiságát valós idejű nyilvántartásokban is;

   írásbeli indoklással visszautasítja a Tanúsítvány kiadását, amennyiben a tanúsítvány igénylés nem teljes, nem helyes, nem az arra jogosult által történik, vagy egyéb módon nem felel meg az elvárt feltételeknek,
6. nyilvántartásba vesz minden, a tanúsítványok kiadásához kapcsolódó, a 2/2002. (IV.26) MeHVM irányelve 152. pontjában és a HSzSz 4.1 pontjában meghatározott információt, kivéve a hivatkozott irányelv 152/f. pontjában foglaltakat,
7. megőrzi a 6. pontbeli nyilvántartásokat a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított tíz évig, illetőleg velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig
8. bizalmas információként kezeli az Előfizető és az Aláíró minden adatát, kivéve azokat, amelyeket a 2.8.2 pont tárgyal. A Szolgáltató a birtokába jutott bizalmas információkat a személyes adatok védelméről szóló 1992 évi LXIII. törvénynek megfelelően kezeli, s csak a 2.8.3-2.8.7 pontokban említett esetekben és személyek részére fedi fel őket,
9. korlátozás nélkül biztosítja az Aláíró számára a rá vonatkozó regisztrációs és egyéb információhoz történő hozzáférést (lásd 2.8.7).

A regisztráló szervezet a visszavonás kezelés szolgáltatás keretén belül:

1. ellenőrzi a Tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmek hitelességét és érvényességét (lásd még 4.4.2 és 4.4.6), valamint szabályosságát lásd még 4.4.3 és 4.4.7),
2. tájékoztatja a visszavont, illetve felfüggesztett Tanúsítvány tulajdonosát Tanúsítványa állapotának változásáról,
3. haladéktalanul, maximum a HSzSz 4.4.4, illetve 4.4.7 pontjában meghatározott időn belül továbbítja a hiteles, érvényes és szabályos, Tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket a regisztráló szervezethez,
4. visszautasítja (az ok megjelölésével) a nem hiteles, érvénytelen, vagy szabálytalan, Tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket,
5. a visszavonási kérelem elfogadása után haladéktalanul, maximum a HSzSz 4.4.4 pontjában meghatározott időn belül intézkedik egy Tanúsítvány visszavonásáról,

6. intézkedik saját Tanúsítványának visszavonása, illetve felfüggesztése végett, amennyiben magánkulcsa kompromittálódott, vagy ennek gyanúja áll fenn,
7. 99.9%-os rendelkezésre állással biztosítja a visszavonás kezelési szolgáltatást minden érdekelt fél számára, egyúttal szolgáltatási szabályzatában megadja az előre tervezett és rendkívüli leállások leghosszabb időtartamát.

A regisztráló szervezet az Aláírás létrehozó adat előállítása szolgáltatás keretén belül:

1. gondoskodik valamennyi általa, az Aláíró számára végrehajtott kulcs előállítás biztonságosságáról, az Aláíró magánkulcsának titkosságáról,
2. olyan algoritmus felhasználásával állítja elő, amelyet a 2/2002. (IV.26) MeHVM irányelv 1. sz. melléklete az elfogadott kriptográfiai algoritmusok között megfelelő kulcs generáló algoritmusként ismer el,
3. olyan aláíró algoritmushoz és olyan kulcshosszúságban állítja elő, melyet a 2/2002. (IV.26) MeHVM irányelv 1. sz. melléklete az elfogadott kriptográfiai algoritmusok között megfelelő aláíró algoritmusként, illetve megfelelő paraméterként ismer el,
4. biztonságos módon eljuttatja az Aláíró részére előállított kulcspárt olyan biztonságos útvonal kiépítésével, mely megfelelő kriptográfiai mechanizmusok felhasználásával forráshitelesítést, sértetlenséget és bizalmasságot biztosít,
5. biztonságos módon megsemmisíti az Aláíró részére előállított magánkulcsot, miután az Aláíróhoz eljuttatta az előállított kulcspárt,
6. biztosítja saját Aláírás létrehozó adatainak biztonságos használatát és tárolását.

A regisztráló szervezet a tanúsítvány előállítás szolgáltatásban való közreműködés keretén belül:

1. kezdeti tanúsítvány előállítás esetén a regisztráció szolgáltatás 3., 4., és 5. pontjaiban leírt módon összegyűjtött, Tanúsítványba kerülő adatokat ellenőrzi az adott tanúsítványtípushoz kapcsolódó hitelesítési, ellenőrzési eljárás szerint,
2. a Tanúsítványhoz tartozó kulcscsere kérelem[7] esetén ellenőrzi a már korábban nyilvántartásba vett Aláírótól érkező tanúsítvány megújítási kérelem teljességét, pontosságát, hitelességét és teljesíthetőségét a HSzSz 3.1 pontjában a kezdeti regisztrációnál meghatározott ellenőrzési módszerrel.

[7] Ez nem vonatkozik a másik két tanúsítvány megújítási formára: a tanúsítványfrissítésre és a tanúsítvány aktualizálásra, ahol a Szolgáltató az Igénylő személyes megjelenését követeli meg.

3. tanúsítvány frissítés esetén a hitelesség ellenőrzéséhez a Szolgáltató nem minden esetben követeli meg az Előfizető vagy az Aláíró ismételt személyes megjelenését, elfogad, illetve feldolgoz minősített elektronikus aláírással hitelesített elektronikus kérelmet is.
4. a Tanúsítvány kibocsátásához szükséges ellenőrzések és visszaigazolások sikeres befejeződése után a hitelesítő szervezet felé tanúsítvány kibocsátási kérelem üzenetet indít el;
5. feldolgozza a teljes, pontos, hiteles és teljesíthető tanúsítvány megújítási kérelmeket az alábbi módon:
   - tanúsítványfrissítés kérelme esetén az Aláíró korábbi Tanúsítványában szereplő adataiból[8] és nyilvános kulcsából összeállítja az aláírandó új Tanúsítványt,
   - tanúsítvány aktualizálás kérelme esetén nyilvántartásba veszi az Aláíró megváltozott új adatait[9], majd visszavonja a régi tanúsítványt és a nyilvántartásba vett adatokból és az Aláíró nyilvános kulcsából összeállítja az aláírandó új Tanúsítványt,
   - tanúsítvány kulcscsere kérelme esetén visszavonja a régi tanúsítványt, majd az Aláíró korábbi Tanúsítványában szereplő adataiból és az új nyilvános kulccsal összeállítja az aláírandó új Tanúsítványt,
6. a tanúsítvány megújítási kérelem sikeres feldolgozása után a hitelesítő szervezet felé tanúsítvány kérelem üzenetet indít el,
7. biztosítja az aláírandó Tanúsítványt is tartalmazó tanúsítvány kérelem üzenet sértetlenségét, hitelességét és bizalmasságát.

A regisztráló szervezet a (Tanúsítvány és szabályzat) kibocsátás szolgáltatásban való közreműködés keretén belül:

1. fogadja a hitelesítő szervezettől kapott új tanúsítványokat, illetve új szabályzatokat, valamint ellenőrzi ezek hitelességét és sértetlenségét,
2. elküldi a Címtárnak az új tanúsítványokat[10], illetve új szabályzatokat, biztosítva az ezt tartalmazó üzenet hitelességét és sértetlenségét.

[8] Egyúttal a regisztráció szolgáltatással együttműködve ellenőrzi, hogy a tanúsítványtulajdonos azonosságának és jellemzőinek igazolására használt információ érvényes-e még.
[9] Egyúttal a regisztráció szolgáltatással együttműködve ellenőrzi, hogy a tanúsítványtulajdonos azonosságának és jellemzőinek igazolására használt új információ érvényes-e.
[10] Amennyiben az Aláíró hozzájárult ehhez.

A regisztráló szervezet a visszavonási állapot közzététele szolgáltatásban való közreműködés keretén belül:

1. rendszeresen új Tanúsítvány visszavonási listát készít tanúsítvány állapot adatbázisából, naponta egyszer, a szolgáltatási szabályzatban meghatározott frissítési időponthoz igazodóan, mely tartalmazza a következő lista tervezett kibocsátási idejét is,
2. rendkívüli esetben[11] új Tanúsítvány visszavonási listát készít tanúsítvány állapot adatbázisából, mely tartalmazza a következő lista tervezett kibocsátási idejét is,
3. aláírás céljából elküldi a hitelesítő szervezetnek az új Tanúsítvány visszavonási listát, (a visszavonási lista aláírási kérelemben), biztosítva az ezt tartalmazó üzenet hitelességét és sértetlenségét,
4. elküldi a Címtárnak az új Tanúsítvány visszavonási listát, biztosítva az ezt tartalmazó üzenet hitelességét és sértetlenségét.

2.1.5. A Címtár feladatok és kötelezettségek

A Szolgáltatónak a hét minden nap napi 24 órában folyamatosan fogadnia és feldolgoznia kell az előfizetőktől a Tanúsítványokkal kapcsolatos változások adatait, nyilvántartást kell vezetnie a Tanúsítványok aktuális helyzetéről, esetleges felfüggesztéséről, illetve visszavonásáról. Ezeket, valamint az aláírás ellenőrző adatokat, továbbá a Visszavont tanúsítványok listáját (CRL) közcélú Internet segítségével bárki számára hozzáférhető és folyamatosan[13] elérhető módon közzéteszi.

A Címtár az alábbi elektronikus aláírással kapcsolatos szolgáltatásokat biztosítja:

- (Tanúsítvány és szabályzat) kibocsátás,
- visszavonási állapot közzététele.

A Címtárat a Szolgáltatónak 99,9 % rendelkezésre állási szinten kell elérhetővé tennie.

A Címtár a kibocsátás szolgáltatás keretén belül:

[11] Rendkívüli esetnek számít a Szolgáltató saját magánkulcsának kompromittálódása, illetve jelentős számú új tanúsítvány visszavonási kérelem beérkezése.

[12] Ez nem vonatkozik a másik két tanúsítvány megújítási formára: a tanúsítványfrissítésre és a tanúsítvány aktualizálásra, ahol a Szolgáltató az Igénylő személyes megjelenését követeli meg.

[13] A hét 7 napján, a nap 24 órájában.

1. közzé teszi az előfizetői tanúsítványokat[14],
2. nyilvánosságra hozza a szolgáltatási szabályzatot, általános szerződési feltételeket és egyéb ezekhez kapcsolódó információt,
3. biztosítja a 2. és a 3. pontokban szereplő információ folyamatos[15] elérhetőségét, még rendkívüli üzemeltetési helyzet esetén is.

A Címtár a visszavonási állapot közzététele szolgáltatás keretén belül:

1. közzé teszi a hiteles és sértetlen új Tanúsítvány visszavonási listát;

   Előfizetői kérelem vagy a Szolgáltató alapos indokkal meghozott döntése alapján történő Tanúsítvány felfüggesztést vagy visszavonást a Szolgáltató belső nyilvántartásában haladéktalanul, de legrosszabb esetben 1 órán belül végre kell hajtani. A felfüggesztés vagy a visszavonás publikálása a legközelebbi közzétételi időpontban történik meg.
2. biztosítja a legfrissebb Tanúsítvány visszavonási lista folyamatos[16] elérhetőségét, még rendkívüli üzemeltetési helyzet esetén is.

Annak érdekében, hogy a Címtár elérési útvonala bárki számára hozzáférhető legyen, Szolgáltató köteles a HSzSz 2.6.4 pontjában, az Előfizetői Szerződésben felsorolni azokat az Internet címeket, ahol a különböző hitelesítő szervezeteknél vezetett nyilvántartások elérhetőek.

A Címtár elérési útvonala produktív hitelesítő szervezetenként változhat. A kibocsátott Tanúsítványokat a kibocsátást követően haladéktalanul közzé kell tenni a Címtárban. A visszavont és felfüggesztett tanúsítványokra vonatkozó közzétételi időpontja, valamint a visszavonási listák frissítésének időintervalluma a HSzSz 2.6.4 pontjában megadott web lap címen érhető el az előfizetők, az aláírók és az érintett felek által.

2.1.6. Az Igénylő, az Előfizető és Aláíró feladatai és hatásköre

[14] Amennyiben az Aláíró hozzájárult ehhez.
[15] A hét 7 napján, a nap 24 órájában.
[16] A hét 7 napján, a nap 24 órájában.

Az Igénylő, az Előfizető, illetve az Aláíró kötelessége a Szolgáltató szerződéses feltételeinek és szabályzatainak megfelelően eljárni a Tanúsítvány és magánkulcs igénylése és felhasználása során, ezen belül köteles:

1. az Előfizető aregisztráló szervezetnél személyesen megjelenő Igénylőt, aki a Tanúsítványt és az ezzel kapcsolatos műveleteket igényelni fogja, meghatalmazással ellátni,
2. az Igénylő a Tanúsítvány igénylése előtt megismerni és elfogadni Szolgáltató általános szerződéses feltételeit és HSzSz-ét,
3. az Előfizető a HSzSz és az Általános Szerződéses Feltételeket az alkalmazásában álló vagy vele szerződéses kapcsolatban álló aláírókkal megismertetni, különösen az elektronikus aláírás biztonságos használatával, technikai feltételeivel és jogi következményeivel kapcsolatosan,
4. a Tanúsítvány igénylését és a kulcs-pár felhasználását úgy végezni, hogy az harmadik fél jogait ne sértse,
5. az Előfizető a Tanúsítvány kiadásához szükséges aláírói adatokat ellenőrizni, ennek érdekében a Tanúsítvány kibocsátására vonatkozó kérelem érvényesítését megelőzően köteles az Aláírót azonosítani,
6. az Előfizető teljes, pontos, valós és hiteles adatokat szolgáltatni a Szolgáltató részére az igényelni kívánt tanúsítványtípus és fajta követelményeinek megfelelően az Aláíró személyazonosságát, szervezeti identitását és a regisztrációhoz szükséges egyéb jellemzőket illetően,
7. az Előfizető és az Aláíró megismerni a Magánkulcsának átvétele és felhasználása előtt a magánkulcs tárolásával, s az elektronikus aláírás megtételével kapcsolatos technikai, jogi, biztonsági követelményeket és feltételeket,
8. az Aláíró biztosítani az Aláírás létrehozó adatának védelmét,
9. az Előfizető az Aláíró figyelmét külön felhívni arra, ha az Előfizetői Szerződés a Tanúsítvány felhasználhatóságával kapcsolatban összeg, területi vagy egyéb korlátozásokat köthet ki;

   az Előfizető az Aláírás létrehozó adatát csak a vele közölt valamennyi korlátozásnak megfelelően használhatja,
10. az Aláíró tudomásul venni, hogy magánkulcsának védelme és az elektronikus aláírás készítése kizárólag a saját felelőssége, ezért ezzel - így különösen a magánkulcsának

illetéktelen harmadik személyhez kerülésével - kapcsolatban a Szolgáltatót semmiféle felelősség nem terheli;

az Aláíró nem jogosult a Tanúsítványban megadott nyilvános kulcs titkos párját újabb Tanúsítványok vagy bármely más formátumú tanúsított kulccsal használni,

11. az Aláíró tájékoztatni az Érintett felet arról, hogy a HSzSz-ben meghatározott aláírás ellenőrzés lépéseinek elmulasztásából eredő következményekért az Érintett félfelel,
12. az Aláíró azonnal, de legkésőbb a HSzSz 2.1.7/10. pontjában meghatározott időn belül intézkedni Tanúsítványának visszavonása, illetve felfüggesztése végett, amennyiben
    - tudomására jut, hogy a Tanúsítványban foglalt adatok nem felelnek meg a valóságnak, tartalmában, a regisztrációs adatokban pontatlanság van, illetve azokban változás következett be,
    - az Aláírás létrehozó adat és/vagy a PIN kód nem az Aláíró kizárólagos birtokában van (elveszett, ellopták, esetleg kompromittálták), vagy ennek alapos gyanúja áll fenn,
13. kompromittálódás esetén az Aláíró magánkulcsának használatát azonnal és véglegesen megszakítani,
14. az Előfizető, illetve az Aláíró a HSzSz 2.1.7/10 pontjában meghatározott időn belül jelezni a Szolgáltatnál a regisztráció során felvett adataiban történő változásokat, különös tekintettel a Tanúsítványba foglalt adatokra,
15. az Előfizető az Előfizetői Szerződésben rögzített szolgáltatási díjakat a Szolgáltatónak megfizetni,
16. az Előfizető az ÁSzF módosításáról szóló értesítést követően, a HSzSz 2.1.7/14 pontjában meghatározott időn belül köteles az aláírókat írásban tájékoztatni a változásokról. Amennyiben az Előfizető nem fogadja el az ÁSzF módosítását, felmondási szándékát a HSzSz 2.1.7/16 pontjában meghatározott időn belül be kell jelentenie írásban az illetékes regisztráló szervezetnél, amely a felmondás beérkezését követő, a HSzSz 2.1.7/16 pontjában meghatározott időpontig kezdeményezi a Tanúsítvány visszavonását,
17. az Aláíró vagy az Előfizető a Tanúsítvánnyal ellátott elektronikus dokumentummal kapcsolatos jogvita megindulásáról köteles haladéktalanul tájékoztatni a Szolgáltatót.

Ezeken kívül:

1. az Aláíró jogosult arra, hogy a magánkulcsot birtokolja és a jogszabályokban meghatározott módon elektronikus aláíráshoz, és más, a HP-ben, a HSzSz-ben és az Előfizetői Szerződésben rögzített tevékenységhez csak (a Tanúsítványban is feltüntetett névmegadás szerint) saját, illetve szervezete nevében felhasználja,
2. az ÁSzF tartalmazza az Előfizetői Szerződésnek az Előfizető, illetve a Szolgáltató által történő rendes vagy soron kívüli felmondásának feltételeit,
3. az Aláíró tudomásul veszi, hogy a magánkulcsával készített elektronikus aláírás a saját elektronikus aláírásának minősül, és viseli ennek jogkövetkezményeit;

   az Aláíró a Tanúsítványt csak a HP-nek, a HSzSz-nek, valamint a hatályos jogszabályi rendelkezéseknek megfelelően használhatja; elektronikus aláírás csak Tanúsítvány érvényességi ideje alatt készíthető,

2.1.7. Érintett fél feladatai és hatásköre

Az Érintett félnek kötelessége Szolgáltató szabályzatainak megfelelően a legnagyobb gondossággal eljárni az elektronikus aláírás és a Tanúsítvány elbírálásakor, ezen belül:

1. Az Elektronikus aláírás elfogadása előtt meg kell értenie az Elektronikus aláírással kapcsolatos technikai, jogi, biztonsági és egyéb vonatkozásokat.
2. Meg kell ismernie Szolgáltató nyilvánosan elérhető szabályzatait (HSzSz, ÁSzF) és az Elektronikus aláírással ellátott dokumentum alapján végzett bármilyen tevékenység a Szolgáltató szabályzatának elfogadását jelenti.
3. Az Elektronikus aláírás ellenőrzését el kell végeznie az Aláíró Tanúsítványának segítségével, meggyőződve az üzenet eredetiségéről és az aláírás valódiságáról.
4. A Tanúsítványban feltűntetett azonosító alapján, és egyéb adatok, törvényesen rendelkezésre álló módszerek segítségével az Aláíró személyéről egyértelműen meg kell győződnie.
5. A Tanúsítvány érvényességét és hatályosságát ellenőriznie kell a nyilvánosan elérhető Tanúsítványban.
6. El kell végeznie a teljes tanúsítási lánc ellenőrzését az alábbiak szerint:
   - A Tanúsítvány kibocsátójának azonosítója alapján a Kibocsátó kilétéről meg kell győződnie.

- A Kibocsátó Tanúsítványának segítségével az Aláíró Tanúsítványának integritásáról meg kell győződnie.
- A Tanúsítvány állapotát ellenőriznie kell a Tanúsítvány visszavonási listák (CRL) áttanulmányozásával.
- Át kell tanulmányoznia a Tanúsítvány összes attribútumát, közöttük a korlátozó feltételeket is, és az adott tranzakcióra vonatkozó előírásoknak, valamint józan megfontolásoknak megfelelően döntést hozni az aláírás elfogadásáról.

7. Az Elektronikus aláírás elfogadását vissza kell utasítani, ha az Elektronikus aláírás, az Aláíró Tanúsítványa, vagy a tanúsítási lánc tanúsítványainak valamely adata, annak érvénytelenségére utal, illetve ha az az adott kontextusban nem elfogadható. Az aláírás elfogadása nem jelenti az aláírt üzenet tartalmának tudomásul vételét vagy elfogadását.

2.2. A hitelesítés szolgáltató és felhasználó közösség tagjainak felelőssége

2.2.1. A MÁV INFORMATIKA Kft. felelőssége

Általános Szabály

A MÁV INFORMATIKA Kft., mint Hitelesítés Szolgáltató azzal, hogy aláír egy, a jelen HP 1.4 pontja szerint meghatározott minősített tanúsítványt – ezzel a Tanúsítvány által tartalmazott információkra támaszkodó, az 1.3 pontban meghatározott felhasználó közösség és az érintett felek felé jelzi ezen HP, valamint a HSzSz használatát –, csak azért vállalja a felelősséget, hogy a tanúsítvány előállítás, kibocsátás, közzététel, visszavonás és Visszavonási Lista közzététel tevékenységek a jelen HP-ben és a HSzSz-ben előírtaknak teljes mértékben megfelelnek és a Szolgáltató megteszi a szükséges intézkedéseket, hogy a regisztráló szervezet és az előfizetők is a jelen HP-nek és a HSzSz-nek megfelelően jártak el.

Amennyiben a Szolgáltató a HSzSz szabályainak vétkes megszegésével kárt okoz azért, a vele szerződéses jogviszonyban nem álló Érintett féllel szemben a Magyar Köztársaság Polgári törvénykönyvéről szóló 1959. évi IV. törvény 339.§-ának megfelelően, a Szerződéses partnerrel szemben pedig a szerződésszegésért való felelősség szabályai szerint felelős a Szolgáltató. A Szolgáltató a szolgáltatásaival

kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben kizárólag a hibájából, kötelezettségeinek megszegéséből, valamint a neki felróható okokból bekövetkező, bizonyítható károkért tartozik helyt állni. Általában a Szolgáltató nem vállal felelősséget, ha a Szolgáltató által kibocsátott Tanúsítvány a jelen HP-ben előírtaktól eltérő módon kerül felhasználásra. Így a Szolgáltató nem felelős az olyan károkért, mely abból adódott, hogy az Érintett fél a tanúsítványok ellenőrzése és felhasználása során nem a hatályos jogszabályok és a Szolgáltató HSzSz-e szerint járt el, illetve nem tanúsította a tőle elvárható gondosságot.

A Szolgáltató felelősségére a következő részletes szabályok mérvadók:

- Amennyiben a HSzSz szabályai megszegésével a Szolgáltató a vele szerződéses jogviszonyban nem álló Érintett félnek kárt okoz, vagy a Tanúsítvány Érintett fél általi, – a HSzSz szerint történő – felhasználása ellenére, az Érintett fél kárt szenved, azért a Magyar Köztársaság Polgári Törvénykönyvéről szóló 1959. évi IV. törvény 339. §-ának megfelelően a Szolgáltató felelős, azzal a korlátozással, hogy a kártérítés mértéke Tanúsítvány típusonként és egyedi tanúsítványonként is maximált összegű az ÁSzF vagy az Előfizetői Szerződés vonatkozó feltételei szerint.
- A Szolgáltató köteles a Tanúsítvány megfelelő mezőjében feltüntetni, ha az Előfizetői Szerződésben a Tanúsítvány felhasználhatóságával kapcsolatban összeg, területi vagy egyéb korlátozásokat köt ki. Ezen korlátokat meghaladó ügyletekben kibocsátott és aláírt elektronikus dokumentumokból származó követelésekért, illetve az így okozott kárért a Szolgáltató nem felel.
- A Szolgáltató a vele szerződéses jogviszonyban álló felekkel (ilyen az Aláíró és az Előfizető) szemben a Polgári Törvénykönyv szerződésszegésért való felelősség szabályai szerint felelős.
- A Szolgáltató felelősséget vállal az általa támogatott tanúsítványtípusokban és fajtákban leírt eljárásoknak való megfelelőségért, még abban az esetben is, amikor a Szolgáltató funkcionalitásait alvállalkozók végzik[17].
- A Szolgáltató kizárja felelősségét, ha az aláírás ellenőrzés lépései a HP-ben meghatározott módon bármi okból – beleértve Szolgáltatónál keletkező üzemeltetési problémát is – nem hajthatóak végre az aláírás ellenőrzésének időpontjában, és az

elektronikus aláírás, illetve az aláírással ellátott dokumentum az aláírás ellenőrzője által ennek ellenére elfogadásra kerül.

- A Szolgáltató által okozott kárral kapcsolatos felelősségi és a kártérítési szabályt a 2.3.1 pont határozza meg.
-
- A Szolgáltató nem vagyoni felelőssége az Előfizető és Érintett fél felé a Polgári Törvénykönyv nem vagyoni felelősségről szóló szabályai szerint alakul.
- A Tanúsítvány lejárat előtti megszüntetése esetén, a kártérítési felelősség korlátozásáról a 2.3.1 pont rendelkezik.

2.2.2. A hitelesítő szervezet felelőssége

A hitelesítő szervezetek felelősségének belső megosztása nem érinti a szolgáltató társaság egységes jogi felelősségét.

Elsődleges (Root) hitelesítő szervezet felelőssége:

- felelős a közvetlenül alá rendelt hitelesítő központok és szervezetek hitelesítésért.
- nem felelős az alá rendelt hitelesítő szervezetek működéséért.

Fizikailag létező produktív hitelesítő szervezet felelőssége:

- felelős az általa kibocsátott tanúsítványok hitelességéért.
- felelős az általa létrehozott alárendelt hitelesítő központok hitelesítésért,
- felelős az alárendelt regisztrációs irodák működéséért.
- nem felelős az előfizetők aláírási és más hitelesítő központok által kibocsátott magánkulcsok és tanúsítványok felhasználási tevékenységért,
- nem felelős az érintett felek aláírás ellenőrzési és Tanúsítvány elbírálási tevékenységért.

2.2.3. Hitelesítési Politika és Szabályozási Csoport felelőssége

A Hitelesítési Politika és Szabályozási Csoport felelős a HP, a HSzSz és a Szolgáltató minden szervezeti egysége által kibocsátott más szabályzatok ellentmondás-mentességéért,

[17] A Szolgáltató általánosan felelős a hitelesítő szervezet, a regisztráló szervezet, valamint a címtár kötelezettségeiért, tevékenységeiért.

megfelelő értelmezhetőségéért és használhatóságáért, azok törvényi megfelelőségéért, érvényesítésért és betartatásáért.

A Hitelesítési Politika és Szabályozási Csoport nem felelős az előfizetők, az érintett felek, és a felhasználó közösség szervezetei által kibocsátott szabályzatokért.

2.2.4. A regisztráló szervezet felelőssége

A regisztráló szervezet felelős:

- az előfizetők személyazonosságának és szervezeti identitásának megállapításáért és a bemutatott dokumentumok alapján történő ellenőrzéséért,
- a felvett regisztrációs adatok valódiságáért,
- a regisztrációs adatoknak a hitelesítő szervezethez történő bizalmas, hiteles és sértetlen eljuttatásáért,
- a Tanúsítvány visszavonási igény bejelentője személyazonosságának és szervezeti identitásának megállapításáért és a bemutatott dokumentumok alapján történő ellenőrzéséért,
- az általa generált kulcspárok megfelelőségéért, az Aláírás létrehozó adat, az Aláírás ellenőrző adat és a Tanúsítvány összetartozásáért és a Tanúsítvánnyal együtt történő Aláírás létrehozó eszközre írásért,
- az Aláírás létrehozó eszköz és az aktivizáló kód összetartozásáért,
- az előfizetői pénzkezelésért.

2.2.5. Az Aláíró és az Előfizető felelőssége

Az Előfizetőnek büntetőjogi felelőssége áll fenn Szolgáltatóval szemben, ha az Aláíró regisztráció során megadott adatai nem valódiak és/vagy nem hitelesek és ezzel a Szolgáltatónak kárt okoz.

Az Előfizetőnek kártérítési felelőssége áll fenn Szolgáltatóval szemben azokért a veszteségekért és károkért, melyeket az Aláíró regisztráció során megadott helytelen adataival, vagy az azokban bekövetkezett változások be nem jelentésével, vagy egyéb kötelezettségeinek be nem tartásával számára okoz. Az Előfizető felelős azért, ha magánkulcsát nem a HSzSz-ben, az Általános Szolgáltatási Feltételekben és a vonatkozó jogszabályokban meghatározott módon és célra használta.

Az Aláíró felelős:

- regisztráció során megadott adatai valódiságáért, pontosságáért és érvényességéért,
- az adatokban bekövetkezett változások bejelentéséért,
- magánkulcsának a szabályzatoknak megfelelő felhasználásáért,
- magánkulcsának és aktivizáló kódjának biztonságáért,
- általában kötelezettségei betartásáért.

A Szolgáltató nem vállal felelősséget a magánkulcs hordozó elvesztéséből, vagy a kulcs biztonságának egyéb módon történő sérüléséből, elvesztéséből, illetve a PIN kód illetéktelen tudomásra jutásból származó károkért.

2.2.6. Érintett fél felelőssége

Érintett fél felelőssége fennáll a Tanúsítvány elfogadásából fakadó bármely következményért és kárért, ha a Tanúsítvány érvényességének és hatályosságának ellenőrzése során nem a tanúsítványtípus, a szolgáltatási szabályzat, illetve a hatályos jogszabályok szerint jár el.

Az Érintett fél felelős az elektronikus aláírás és a Szolgáltató által kibocsátott tanúsítványok elfogadása során tanúsított körültekintő ellenőrzésért, valamint a Szolgáltató nyilvánosan elérhető HSzSz-e rá vonatkozó részének megismerésért, a 2.1.7 pontban meghatározott kötelezettségeinek betartásáért.

Az Érintett fél felelőssége fennáll, ha a Tanúsítvány érvényességének és hatályosságának ellenőrzése során nem a HSzSz, illetve a hatályos jogszabályok szerint jár el.

2.3. Az anyagi felelősség korlátjai

2.3.1. Kártérítés

Amennyiben a Szolgáltató a HSzSz, illetve a jelen HP szabályainak vétkes megszegésével kárt okoz azért, a vele szerződéses jogviszonyban nem álló Érintett féllel szemben a 2.2.1 pontban meghatározottak szerint felelős. A kártérítés mértéke káreseményenként maximált összegű az ÁSZF 5.1.1. pontjának előírásai szerint.

A Szolgáltató nem felelős az olyan kárért, amely abból adódott, hogy az Érintett fél a tanúsítványok, illetve az elektronikus aláírások hitelességének ellenőrzésénél nem a hatályos jogszabályok és a HSzSz szerint járt el, illetve nem tanúsította a tőle elvárható gondosságot.

Az Aláírás létrehozó adat, illetve eszköz illetéktelen kezekbe kerülés esetén a Szolgáltató nem felelős egészen az Előfizető vagy Aláíró által tett bejelentés időpontjáig azért a kárért, amely abból származik, hogy az Előfizető, illetve az Aláíró nem a HP-ben előírt biztonságos feltételek mellett tárolta, használta az Aláírás létrehozó adatot, illetve eszközt, és emiatt az illetéktelen felhasználásra került. Az előfizetők és az érintett felek kártérítési felelősséggel tartoznak a Szolgáltatóval szemben azokért a veszteségekért és károkért, amelyeket kötelezettségeik be nem tartásával okoznak számára.

A Szolgáltató felelősségének összegszerű felső határát – amennyiben az Előfizetői Szerződésben a Felek másként nem állapodnak meg - az ÁSZF 5.1.1. pontja tartalmazza. Szolgáltató – helytállási kötelezettsége esetén – csak a Szerződésben, illetve a Tanúsítványban megjelölt összeghatárig köteles kártérítésre.

A Szolgáltatással kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben a Szolgáltató a hibájából, kötelezettségeinek megszegéséből, neki felróható okból bekövetkező és bizonyított közvetlen károkért tartozik helytállni.

A Szolgáltató megfelelő megoldásokkal rendelkezik a műveleteiből és tevékenységeiből származó kötelezettségek fedezésére, különösképpen a kárfelelősség kockázatára vonatkozóan.

A Szolgáltató rendelkezik a jelen dokumentumban foglaltakkal összhangban álló üzemeltetéshez szükséges pénzügyi stabilitással és erőforrásokkal.

2.3.2. Megbízotti kapcsolatok

Azáltal, hogy a Szolgáltató az előfizetők részére tanúsítványokat bocsát ki, semmilyen körülmények között nem tekinthető az előfizetők vagy az érintett felek ügynökének, megbízottjának, képviselőjének, vagy bármilyen más, az Előfizetői Szerződésben meghatározottól eltérő funkciójú partnerének a hitelesítési tevékenysége vonatkozásában.

2.3.3. Adminisztratív eljárások

A Szolgáltató a vagyoni felelősségre vonhatóság, az általa okozott károkkal kapcsolatos saját felelősség, illetve a neki okozott károkért járó kártérítés megállapíthatósága, dokumentálása és bizonyíthatósága érdekében naplózza tevékenységeit, védi a naplóbejegyzések sértetlenségét és hitelességét, valamint hosszú távon megőrzi (archiválja) azokat. (Részletesebben lásd a 4.5 és 4.6 alfejezeteket.)

2.4. Értelmezés és alkalmazás

2.4.1. Irányadó jog

A Szolgáltató tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi. Szerződéseire és szabályzataira, és azok teljesítésére, a magyar jog az irányadó, és azok a magyar jog szerint értelmezendők.

A Szolgáltató tevékenységére elsősorban a következő jogszabályok mérvadók:

- 2001. évi XXXV. törvény az elektronikus aláírásról[18]
- 100/2000. (VI. 23.) Korm. rendelet az információs társadalom megvalósításával összefüggő feladatokról, az informatikai kormánybiztos feladat- és hatásköréről
- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.
- 1014/2001. (III.5.) Korm. határozat az elektronikus aláírásról szóló törvény alapelveiről és az ezzel kapcsolatban szükséges intézkedésekről szóló 1075/2000. (IX.13.) Korm. határozat módosításáról.
- 151/2001. (IX. 1.) Kormányrendelet a Hírközlési Felügyeletnek az elektronikus aláírással kapcsolatos feladat-és hatásköréről, valamint eljárásainak részletes szabályairól.
- 20/2001. (XI.15.) MeHVM rendelet a Hírközlési Felügyeletnek az elektronikus aláírással összefüggő minősítéssel nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról.
- 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.

[18] A törvényt kiegészítő, alább felsorolt alacsonyabb szintű jogszabályok a 2002 május 31.-i állapotot tükrözik.

- 2/2002. (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről.
- 15/2001. (VIII. 27.) MeHVM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról.
- 1026/2002. (III. 26.) Kormányhatározat a kormányzati elektronikus aláírási rendszer kiépítésével összefüggő egyes feladatokról és a kormányzati központi kormányzati hitelesítés-szolgáltató felállításáról.
- *47*/2002. (III. 26.) Korm. rendelet a kormányzati elektronikus aláírási rendszer kiépítésével összefüggő egyes kormányrendeletek módosításáról
- *7*/2002 (IV.26) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről.

Ezeken túlmenően a Szolgáltató

- az üzleti titkok vonatkozásában az 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról,
- a személyes adatok vonatkozásban az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról és az 1995. évi CXXII. törvény a polgárok személyes adatainak nyilvántartásáról szóló 1992. évi LXVI. tv. Módosításáról

szerint jár el.

Szolgáltató figyelembe veszi még

- az Európai Parlament és Európa Tanács az elektronikus aláírások közösségi programjáról szóló 1999/93/EK irányelvét,
- a vonatkozó ITU szabványokat, az Internet közösség RFC ajánlásait,
- az Európai Unió Távközlési Szabványok Intézetének (ETSI) vonatkozó szabványait.

2.4.2. Érvénytelenség, hatályosság, megszűnés, értesítések

2.4.2.1. Érvénytelenség

Amennyiben a Szolgáltató szerződéseinek vagy szabályzatainak valamely pontja érvénytelenné vagy érvényesíthetetlenné válna, az az egész szabályzat vagy szerződés egyéb pontjainak érvényességét nem érinti.

A jelen HP minden olyan rendelkezése, amely a felelősségek, a kötelezettségek, garanciák és a kártérítés korlátaira vonatkoznak, azok függetlenül más intézkedésektől, önmagukban értelmezendők és érvényesítendők.

2.4.2.2. Hatályosság, fennmaradás

Jelen HP időbeli hatálya az 1.3.5.1 pontnak megfelelően a Hírközlési Felügyelet engedélyének keltétől a szolgáltatási tevékenység megszűntéig tart. A HP személyi és tárgyi hatályát az 1.3.5.1 pont tartalmazza.

Jelen HP 2. fejezete érvényben marad a HP hatályának végét követően is (a hatályosság megszűnésének módjától függetlenül) mindazon tanúsítványokkal kapcsolatosan, melyet jelen tanúsítványtípus hatálya alatt bocsátott ki a Szolgáltató.

2.4.2.3. Megszűnés

Jelen HP a közösség résztvevőinek valamennyi kötelezettségét, felelősségét és jogát tartalmazza. A HP egyetlen pontja sem értelmezhető a jelen dokumentumba foglalt értelmezéstől eltérően, bármely más szerződés vagy szabályzat, írott vagy szóbeli kommunikáció következtében, beleértve a Szolgáltató és más szervezet jövőbeli esetleges összeolvadásának esetét is. A HP csak írott és hitelesített formában módosítható, a Hírközlési Felügyelet által vezetett tanúsítványtípus nyilvántartásban való átvezetés mellett.

A jelen HP a Szolgáltató működésének befejezésével tekintendő megszűntnek.

2.4.2.4. Értesítések

Az előfizetők, az érintett felek vagy bármely harmadik fél a regisztráló szervezetet a HSzSz 2.4.2.4 pontjában megadott időben keresheti meg személyesen telefonon, írásban, e-mail-ben vagy faxon. Naponta 24 órás szolgálattal áll rendelkezésre telefonos vagy e-mail megkeresés esetén a Szolgáltató Help Desk-je. Az írásban vagy elektronikus úton történő kommunikáció esetében a feladó nevét és elérhetőségét fel kell tüntetni és a feladónak a küldeményt hitelesítenie kell.

A Szolgáltató az előfizetőket és érintett feleket tipikusan a web oldalain, illetve az Ügyfélszolgálaton történő közzététellel tájékoztatja. Az előfizetőket esetenként írásban vagy elektronikus úton is értesítheti.

2.4.3. Vitás kérdések kezelése

Bármely vitás kérdés felmerülése esetén az Előfizetőnek, az Érintett félnek, vagy bármely harmadik félnek kötelessége a Szolgáltató haladéktalan értesítése és teljes körű tájékoztatása a kérdés minden vonatkozását érintően, a vita jogi útra terelése előtt.

Panaszt az Előfizetőt nyilvántartó Szolgáltató regisztráló szervezeténél vagy a Help Desknél lehet írásban vagy szóban előterjeszteni az 1.5.2 pontban megadott elérhetőségekkel és időpontokban. A panasz előterjesztésétől számított 10 munkanapon belül a Szolgáltatónak azt ki kell vizsgálnia és írásban kell válaszolnia.

A szerződő feleknek kölcsönösen meg kell állapodnia abban, hogy jogvitáikat mindenkor megkísérlik békés úton tárgyalások útján rendezni. Amennyiben ez az egyeztetés kezdetétől számított 30 napon belül nem vezet eredményre, arra az esetre a Feleknek kölcsönösen alá kell vetniük magukat a Magyar Kereskedelmi és Ipar Kamara mellett szervezett Állandó Választott Bíróság kizárólagos hatáskörének. A Választott Bírósági eljárás nyelve a magyar, az eljárásban irányadó jog a mindenkor hatályos magyar anyagi és eljárásjog.

A jelen HP-ben nem szabályozott kérdésekben a mindenkor hatályos magyar jogszabályok rendelkezései irányadók, különös tekintettel a Polgári Törvénykönyv, az elektronikus aláírásról szóló 2001. évi XXXV. törvény, az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról, valamint az 1995. évi CXXII. törvény a polgárok személyes adatainak nyilvántartásáról szóló 1992. évi LXVI. törvény módosításáról törvények rendelkezésire. Jelen HP-ben szereplő kifejezéseket és jogintézményeket a magyar nyelv szabályi szerint, a szavak általánosan elfogadott mindennapi jelentése szerint, valamint a magyar jogszabályok alapján kell értelmezni.

2.5. Díjak

A mindenkor érvényes szolgáltatási díjakat a Szolgáltató a „http://www.mavinformatika.hu/ca/" web oldalon teszi közzé. A Szolgáltató jogosult az árlistát egyoldalúan módosítani. A módosítást Szolgáltató köteles a fenti web oldalon közzétenni. Az előfizetőkre vonatkozó hatályos szolgáltatási díjak az Előfizetői Szerződésben kerülnek rögzítésre.

A módosított árlista a közzétételt illetve az értesítést követő 20. napon lép hatályba. Azok az előfizetők, akik a módosítást nem fogadják el, jogosultak az Előfizetői Szerződésüket legkésőbb a módosítás életbe lépésének napjáig 10 napos felmondási idővel felmondani. A szerződés felmondása egyben a kiadott Tanúsítvány iránti visszavonási kérelemnek is tekintendő és a Szolgáltató jogosult a Tanúsítványt az adatbázisából törölni.

A Szolgáltató a következő pontokban ismertetett díjtípusokat ajánlja fel az Előfizetőnek.

2.5.1. Tanúsítvány kibocsátás és megújítás

Lásd HSzSz 2.5.1 pont!

2.5.2. Tanúsítvány hozzáférés

Lásd HSzSz 2.5.2 pont!

2.5.3. Visszavonás és állapot információ hozzáférés

Lásd HSzSz 2.5.3 pont!

2.5.4. Egyéb szolgáltatásokra vonatkozó díjak

Lásd HSzSz 2.5.4 pont!

2.5.5. Visszatérítési elvek

Lásd HSzSz 2.5.5 pont!

2.6. Közzététel és Címtár

2.6.1. Szolgáltatói információk közzététele

A Szolgáltató gondoskodik arról, hogy kikötései és egyéb feltételei az előfizetők és az érintett felek rendelkezésére álljanak. Különösképpen:

A Szolgáltató az előfizetők és az érintett felek rendelkezésére bocsátja a tanúsítványok használatára vonatkozó kikötéseket és feltételeket, köztük az alábbiakat:

- az alkalmazott tanúsítványtípus, beleértve egy egyértelmű nyilatkozat arra vonatkozóan, hogy a tanúsítványtípus a nyilvánosság részére kibocsátott tanúsítványokra vonatkozik, és hogy megköveteli-e bármilyen speciális termék, alkalmazás vagy eszköz használatát a kibocsátandó tanúsítvánnyal összekapcsolt kulcspár alkalmazására,
- a tanúsítványok használatára vonatkozó bárminemű korlátozás,
- az Előfizető kötelezettségei a 2.1.6 alfejezetben meghatározottaknak megfelelően,
- a Tanúsítvány ellenőrzésének miként jére vonatkozó információ, beleértve a tanúsítvány visszavonási állapot ellenőrzésére vonatkozó követelményeket, oly módon, hogy az Érintett fél "ésszerű módon hagyatkozhasson" a Tanúsítványra (lásd 2.1.7),
- a felelősségvállalásra vonatkozó bármilyen korlátozást, beleértve azokat az okokat/ használatokat, amelyek esetén a Szolgáltató elfogadja, illetve visszautasítja a felelősség vállalását (lásd 2.3),
- az az időtartam, amíg a regisztrációs információt (lásd 4.6) megőrzik,
- az az időtartam, amíg a Szolgáltató eseménynaplóját (lásd 4.5.3) megőrzik,
- reklamációkra és viták rendezésére vonatkozó eljárások (lásd 2.4.3),
- az alkalmazandó jogi rendszer (lásd 2.4.1) és
- az, hogy a Szolgáltatónak az adott tanúsítványtípusnak való megfelelősége értékelésre került-e, s hogy ez milyen tanúsító rendszeren keresztül történt (lásd 2.7).

A Szolgáltató elérhetővé teszi az előző pontban meghatározott információkat web oldalain keresztül, közérthetően megfogalmazva, elektronikusan továbbítható formában.

Tanúsítványok nyilvánosságra hozatala keretében a Szolgáltató gondoskodik arról, hogy a tanúsítványok szükség esetén az ügyfelek (előfizetők, aláírók és az érintett felek) rendelkezésre álljanak. Részletesebben:

- az előállítás után a teljes és pontos Tanúsítvány rendelkezésre áll azon Előfizető vagy Aláíró számára, akinek a Tanúsítvány kibocsátásra került;
- a tanúsítványok csak azokban az esetekben érhetők el más számára, ha az Előfizető és az Aláíró hozzájárult ehhez;
- a Szolgáltató az érintett felek rendelkezésére bocsátja a Tanúsítvány használatával kapcsolatos kikötéseket és feltételeket;

- egy adott tanúsítvánnyal kapcsolatban a vonatkozó kikötések és feltételek könnyen azonosíthatók.

A Tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatala keretében a Szolgáltató gondoskodik arról, hogy hiteles és érvényes Tanúsítvány visszavonási kérelmek esetén a tanúsítványok időben visszavonásra, s ezen információ nyilvánosságra kerüljön. Részletesebben:

- a Szolgáltató szolgáltatási szabályzatában dokumentálja a tanúsítványok visszavonásának eljárásait, beleértve az alábbiakat:
  - a visszavonási állapot információk nyilvánosságra hozatalánál használt mechanizmusok,
  - a legnagyobb késedelem a visszavonási kérelem fogadása, és az összes érintett fél rendelkezésére álló információk állapotának megváltozása között;
- tájékoztatja a visszavont, illetve felfüggesztett Tanúsítvány tulajdonosát (ahol ez alkalmazható, az Előfizetőt is) Tanúsítványa állapotának megváltozásáról,
- biztosítja, hogy a tanúsítvány visszavonási listákra teljesüljenek az alábbiak:
  - minden egyes visszavonási lista tartalmazza a következő visszavonási lista kibocsátási időpontját,
  - új visszavonási lista közzétehető a következő visszavonási lista kibocsátására megadott időpont előtt is,
  - a visszavonási listát a hitelesítő szervezet a Szolgáltató nevében elektronikusan aláírja.

2.6.2. A közzététel gyakorisága

A Szolgáltató a kibocsátott tanúsítványokat a Címtárban publikálja a 2.6.4 pontban megadott elérhetőséggel. A Tanúsítvány visszavonási listát a HSzSz 4.4.9 pontjának megfelelő gyakorisággal tesz közzé.

A Szolgáltatónak a HP-ben és az ÁSzF-ben tervezett változásokról a hatályba lépést megelőzően 30 nappal tájékoztatnia kell a Hírközlési Felügyeletet, s a változásokkal egységes szerkezetbe foglalva közzé kell tennie, egyéb nyilvános szabályzatait pedig a hatályba lépést megelőző 30 nappal nyilvánosságra kell hoznia.

A Szolgáltató az egyes tanúsítványok nyilvánosságra hozatala kapcsán a HSzSz 2.6.2 pontjában leírt gyakorlatot követi.

2.6.3. Elérési szabályok

A Szolgáltató a nyilvánosságnak bocsát ki Tanúsítványt, ezért a tanúsítványok, valamint a tanúsítványok használatára vonatkozó kikötések és feltételek nyilvánosak, szabványos felületen bárki által elérhetők.

A Szolgáltató minden Előfizető és Érintett fél számára elérhetővé teszi web oldalait és Címtárát olvasás céljából. A Címtárban keresési lehetőséget biztosít a Tanúsítvány sorszáma és az azonosítója alapján. A Címtár és a web oldalak tartalmát csak és kizárólag a Szolgáltató módosítja.

A visszavonásra vonatkozó kérelmeket hitelesíteni kell, a Szolgáltató feldolgozás előtt ellenőrzi, hogy hiteles forrásból származnak-e. Az ilyen jellegű kérelmeket meg kell erősíteni.

A Szolgáltató a nyilvánosságnak bocsát ki Tanúsítványt, ezért a visszavonási állapotokat tartalmazó tanúsítvány visszavonási listák nyilvánosak, szabványos felületen bárki által elérhetők.

A Szolgáltató belső adatbázisait és egyéb adatállományait csak és kizárólag a Szolgáltató Biztonságpolitikája és Biztonsági Szabályzata által meghatározott szerepkörű és jogosultságú munkatársai érhetik el egyénileg differenciált erős azonosítás-hitelesítési és feljogosítási eljárás után.

2.6.4. Címtár

A Szolgáltató a tanúsítványokat, a tanúsítványok használatára vonatkozó kikötéseket és feltételeket, valamint a tanúsítvány visszavonási listákat Címtárán keresztül teszi hozzáférhetővé.

Az Aláíró vagy az Érintett fél a **http://www.mavinformatika.hu/ca/** web lapon keresztül érheti el a Címtár adatokat.

2.7. A megfelelőség vizsgálata

A Szolgáltatót minősített szolgáltatóként 2003. ……..-án lett a Hírközlési Felügyelet által nyilvántartásba véve.
A Hírközlési Felügyelet a Szolgáltató bejelentése alapján a jelen dokumentumban megnevezett tanúsítványtípust nyilvántartásába felvette.

A Szolgáltató olyan elektronikus aláírási termékeket használ „elektronikus aláírás hitelesítés-szolgáltatás" szolgáltatásához (kulcspárok előállításához, a kibocsátott tanúsítványok és tanúsítvány visszavonási listák aláírásához, valamint az ehhez szükséges magánkulcsok tárolásához), amely szerepel a Hírközlési Felügyelet „tanúsított elektronikus aláírási termékek" listáján.

A Szolgáltató az „aláírás létrehozó eszközön az aláírás létrehozó adat elhelyezése" szolgáltatásához olyan aláírás létrehozó eszközt használ fel, mely szerepel a Hírközlési Felügyelet „tanúsított elektronikus aláírási termékek" listáján.

A Szolgáltató a hitelesítő tevékenységét és a hitelesítés szolgáltatást támogató informatikai rendszer, valamint annak személyi és fizikai környezetének biztonságát a HSzSz 2.7 pontjában leírtaknak megfelelően auditáltatja.

2.7.1. Vizsgálatok gyakorisága

A Szolgáltató vonatkozó követelményeknek, valamint a tanúsítványtípusnak való megfelelőség rendszeres felülvizsgálata érdekében a Hírközlési Felügyelet évente legalább egyszer átfogó helyszíni ellenőrzést tart a Szolgáltatónál.

A Szolgáltató által felhasznált elektronikus aláírási termékek megfelelőség vizsgálatának gyakoriságát, illetve egyéb más megfelelőségi vizsgálatok gyakoriságát a HSzSz 2.7.1 pontja határozza meg.

2.7.2. Az átvizsgáló szervezet megnevezése/jellemzői

A minősített Szolgáltatóra vonatkozó követelményeknek, valamint a tanúsítványtípusnak való megfelelőség vizsgálatát a Hírközlési Felügyelet végzi.

A Szolgáltató által felhasznált elektronikus aláírási termékek megfelelőség vizsgálatát, illetve tanúsítását végző szervezeteket a HSzSz 2.7.2 pontja határozza meg.

2.7.3. Az átvizsgáló szervezet és a vizsgált fél kapcsolata

A belső auditot a Szolgáltató hitelesítés szolgáltatást végző szervezeti egységétől független szervezeti egységnek, a külső auditot a Vizsgált féltől, valamint a nyilvános kulcsú infrastruktúra illetve informatikai biztonsági termék és szállítótól független külső auditor cégnek szabad csak elvégeznie.

2.7.4. A vizsgálatok kiterjedése

A vizsgálat a Szolgáltató tanúsítványtípusának és saját szabályzatainak (köztük a HSzSz-nek) való megfelelőség vizsgálatára irányul.

2.7.5. Hiányosságok kezelése

A Hírközlési Felügyelettől rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat a Szolgáltató késlekedés nélkül megszünteti a vizsgálatot végző Hírközlési Felügyelettől kapott információ és ajánlások alapján.

A Szolgáltató által kezdeményezett auditok esetén a hiányosságok kezelését a HSzSz 2.7.5 pontja írja le.

2.7.6. Tájékoztatás az eredményekről

A HSzSz 2.7.6 pontja szerint.

2.8. Bizalmasság – Adatkezelési szabályzat

A Szolgáltatónak gondoskodnia kell a jogszabályoknak való megfelelésről. Ennek keretén belül:

- A fontos bejegyzéseket védi az elveszéstől, tönkretételtől és hamisítástól. A jogszabályoknak való megfelelés, valamint az alapvető üzleti tevékenységek támogatása érdekében szükség van bizonyos bejegyzések biztonságos megőrzésére is. (lásd 4.5 és 4.6),

- gondoskodik az adatvédelmi törvényeknek való megfelelésről,
- megfelelő technikai és szervezeti intézkedéseket hoz a személyes adatok felhatalmazás nélküli, illetve törvénytelen kezelése ellen, valamint a személyes adatok véletlen elveszése, megsemmisülése, illetve károsodása ellen,
- nyilvántartásba veszi az Előfizetővel aláírt megállapodást, beleértve az alábbiakat:
  - hozzájárulás az alábbi szolgáltatások során felhasznált információ a Szolgáltató által történő nyilvántartásba vételéhez: regisztrálás, az aláírók eszközzel való ellátása, esetleges későbbi visszavonás,
  - hozzájárulás a nyilvántartásba vett információ harmadik félhez történő továbbításához, a Szolgáltató szolgáltatásainak leállítása esetén, az erre az esetre vonatkozó szabályzat megkövetelt feltételei szerint,
  - hogy az Előfizető megköveteli-e és az Aláíró hozzájárul-e a Tanúsítvány közzétételéhez és milyen feltételek mellett,
- gondoskodik arról, hogy a regisztrációs eljárás során az adatvédelmi jogszabályok követelményeit figyelembe vegyék,
- ellenőrzési politikája csak annyi bizonyítékot követel meg az azonosításhoz, mely elégséges a Tanúsítvány tervezett felhasználásához,
- gondoskodik az Aláíróra vonatkozó információ bizalmas kezeléséről, kivéve, ha felfedésükhöz ők maguk[19] hozzájárulnak, vagy ha bíróság, illetve egyéb jogi követelmény ezt előírja,
- védi a regisztrációs adatok bizalmasságát (és sértetlenségét) az Előfizetővel/Aláíróval folytatott, illetve a hitelesítő szervezet – regisztráló szervezet – Címtár rendszerkomponensek közötti adatcsere során is.

2.8.1. Bizalmas információk

A Szolgáltató bizalmas információként kezeli az Előfizető és az Aláíró minden adatát, kivéve azokat, amelyeket a 2.8.2 alfejezet tárgyal.

A Szolgáltató a birtokába jutott bizalmas információt a személyes adatok védelméről szóló 1992 évi LXIII. törvénynek megfelelően kezeli, s csak a 2.8.3 - 2.8.7 alfejezetekben említett esetekben és személyek/szervezetek részére fedi fel őket.

A Szolgáltató ezen kívül bizalmas információként kezeli a következő adatokat és dokumentumokat:

- magánkulcsok és aktivizáló kódok,
- tanúsítványigénylések és előfizetői szerződések,
- tranzakciós és napló adatok,
- nem nyilvános szabályzatok,
- minden olyan adat, amelynek nyilvánosságra kerülése a szolgáltatás biztonságát előnytelenül befolyásolná.

2.8.2. Nem bizalmas információk

A Szolgáltató nem bizalmas információként kezeli mindazon adatokat, melyet a Tanúsítványba belefoglal[20]. Ezek az adatok a tanúsítványigénylő űrlapon egyértelműen jelölve vannak.

2.8.3. Tanúsítvány visszavonási és felfüggesztési okok felfedése

A Szolgáltatónak az általa kibocsátott tanúsítványok visszavonását és felfüggesztését Tanúsítvány visszavonási listákban (CRL[21]) kell közzé tennie.

A Szolgáltató a Tanúsítvány visszavonás okát feltünteti a visszavonási listában. Ezen kívül a visszavonással kapcsolatos minden egyéb információt, adatot bizalmasan kezel.

2.8.4. Információszolgáltatás törvényi meghatalmazással rendelkezők részére

A Szolgáltató az elektronikus aláírás felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből – az érintett személyazonosságát igazoló adatok tekintetében - a 2001. évi XXXV. törvény 11.§ alapján adatokat továbbít a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak. Az adatátadás tényét rögzíteni kell, az adatátadásról a Szolgáltató az Aláírót nem tájékoztathatja.

[19] vagy nevükben az Előfizető
[20] Függetlenül attól, hogy az Előfizető hozzájárul-e (az Aláíró nevében) a tanúsítvány nyilvánosságra hozásához.

2.8.5. Információszolgáltatás polgári eljárás keretében

A Szolgáltató a Tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során – az érintettség igazolása esetén – az ellenérdekű peres félnek vagy képviselőjének feltárhat bizalmas felhasználói információkat, illetőleg azokat közölheti a megkereső bírósággal a 2001. évi XXXV. törvény 11.§ (3) bekezdése szerint.

A Szolgáltató rögzíti az információszolgáltatás tényét, és arról tájékoztatja az Előfizetőt és az Aláírót.

2.8.6. Információszolgáltatás tulajdonos kérésére

A Szolgáltató a törvényi meghatalmazással rendelkezők részére történő adatszolgáltatáson túl más Társaság üzleti titkát, az előfizetők és az aláírók nem nyilvános személyes adatait csak az illető Társaság, illetve Előfizető írásos (hagyományos vagy elektronikus aláírással ellátott) meghatalmazása alapján tárhatja fel harmadik fél részére.

Az Aláíró hozzáférhet a rá vonatkozó regisztrációs és egyéb információhoz.

2.8.7. Feltárás más esetekben

A Szolgáltatónak tevékenysége befejezésekor nyilvántartásait, a bizalmas adatokkal együtt, át kell adnia más - vele azonos besorolású – szolgáltató részére a 2001. évi XXXV. törvény 16. § (2.) bek. szerint.

2.9. Szellemi tulajdonhoz fűződő jogok

A Szolgáltató által ügyfelei részére kibocsátott Tanúsítvány és az ennek megfelelő kulcspár tulajdonosa az Előfizető, teljes jogú használója pedig az Aláíró, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat.

A Szolgáltató a Tanúsítványt a kikötéseiben és feltételeiben ismertetett módon közzéteheti, sokszorosíthatja, visszavonhatja, s egyéb módon kezelheti.

A visszavonási információ a Szolgáltató tulajdonát képezi.

[21] CRL: Certification Revocation List

A Szolgáltató által az Aláíró részére kibocsátott egyedi azonosító a Szolgáltató tulajdonát képezi.

A Tanúsítványban szereplő megkülönböztető név használatára a megnevezett Aláíró jogosult.

Az Aláíró egyedi azonosítójában szereplő bármilyen védjegy, szervezeti és személynév, egyéb adat az Előfizető vagy Aláíró tulajdonát képezheti.

A Szolgáltató szabályzatai, szerződéses feltételei a Szolgáltató tulajdonát képezik.

A Tanúsítványban szereplő hitelesítő azonosító a Szolgáltató tulajdonát képezi.

3. Azonosítás és hitelesítés

3.1. Kezdeti regisztráció

A Szolgáltatónak a kezdeti regisztrálás során:

- gondoskodnia kell arról, hogy az Előfizető tanúsítvány kérelmei pontosak, hitelesek és teljesek legyenek,
- megfelelő, illetékes források igazolásán alapulva meg kell vizsgálnia az aláírók és előfizetők azonosságára vonatkozó bizonyítékokat, valamint nevük és a hozzá kapcsolódó adatok pontosságát.

3.1.1. Nevek típusa

A tanúsítványokban szereplő nevek foglalt név (Hitelesítés szolgáltató, illetve Aláíró név) megadásnak az ITU-T X.500 „Information Technology - Open Systems Interconnection - The directory: Overview of concepts, models and services" ajánlása (továbbiakban X.500) egyedi név formátum (Distinguished Name form) előírásainak kell megfelelnie.

A Szolgáltató más név mezőt (pl. Issuer Unique Identifier, Subject Unique Identifier, Issuer Alternative Name, Subject Alternative Name, stb.) nem tölt ki, és nem kezel.

A Tanúsítvány kibocsátójának és a tulajdonosának névmegadását a HSzSz 3.1.1 pontja tartalmazza.

3.1.2. Név jelentése, szemantikája

A Tanúsítványban szerepeltetendő nevek megadásakor a következő szabályok szerint kell eljárni:

- a Szolgáltató a Tanúsítványban álnév feltüntetését vállalja,
- az azonosító nem tartalmazhat olyan speciális karaktereket, amelyek megjelenítése az általánosan használt ügyfél alkalmazásokban nem lehetséges helyesen,
- az azonosító mezői esetében a magyar ABC ékezetes karakterei helyett azok ékezet nélküli megfelelőit kell használni.

3.1.3. Különböző név formátumok értelmezése

A nevek formátumát az 1.4.3 fejezetben meghatározott tanúsítványfajták névmegadási szabályai szerint kell megadni.

3.1.4. Nevek egyedisége

Az Aláíró nevének egyedinek és egyértelműen megkülönböztethetőnek kell lennie a Szolgáltató Címtárában szereplő tanúsítványokban. A Szolgáltatónak biztosítania kell, hogy teljes működési ciklusa alatt egy Tanúsítványban általa használt megkülönböztetett nevet sohasem fogja egy másik egyedhez rendelni.

3.1.5. Név igénylési viták feloldása

Az Aláírót egyértelműen a Tanúsítványban megadott név és a Tanúsítvány sorozat száma különbözteti meg a többi Aláírótól. Ezen kívül a névmegadásnál a Common Name mezőben az Aláíró neve mellett az e-mail címet is meg kell adni, annak érdekében, hogy biztosított legyen a név megkülönböztetés, arra az esetre, ha Tanúsítvány sorozat száma és az Aláíró neve nem elég ehhez.

Amennyiben ez sem elég az egyértelmű név megkülönböztetéshez a Szolgáltató fenntartja magának a jogot a név olyan megváltoztatására, amely továbbra is jellemző az Aláíróra, de biztosítja a megkülönböztethetőséget. Ha az Előfizetőnek az így kiosztott azonosító nem felel meg, akkor kérheti eltérő (a Szolgáltató szabályzatainak megfelelő) azonosító bejegyzését is.

Az Előfizetőnek egy bizonyos azonosítóra való igényét a tanúsítványkérelemben kell jeleznie. Az előfizetői azonosítók kiosztása a beérkezett tanúsítványkérelmek elbírálásának sorrendje szerint történik. Ha a kérelmezett azonosító már korábban kiosztásra került, a Szolgáltató az egyediséget szolgáló eljárásait követve eltérő azonosítót oszt ki.

A Szolgáltató – lehetőségei szerint – a névkiosztás során ellenőrzi az Aláíró jogosultságát a feltüntetett nevek használatára. Szolgáltató fenntartja magának a jogot az igényelt nevek kiosztásának visszautasítására. Jogszerűtlen név- vagy adathasználat miatt, amennyiben erre bíróság kötelezi, vagy másik fél megalapozott módon bizonyítani tudja jogosultságát, a Szolgáltatónak jogában áll visszavonni a kérdéses Tanúsítványt.

3.1.6. Márkanevek elismerésének és hitelesítésének módszere

A tanúsítványkérelemmel az Előfizetőnek kifejezi, hogy a benne foglalt nevek, védjegyek, egyéb adatok nem sértik harmadik fél jogait. Szolgáltatónak nem kötelessége a védjegyek jogos használatának ellenőrzése, és nem vállal közvetítő vagy döntnöki szerepet ilyen jellegű viták feloldásában. Szolgáltató nem garantálja előfizetők számára védjegyeik feltüntetését a Tanúsítványban. Előfizető részéről egy védjegy megszerzése nem tekintendő olyan eseménynek, mely alapján a Tanúsítvány megújítását kell, hogy kezdeményezze.

A tanúsítvány Kibocsátó azonosítója a „Trust&Sign" védjegyet tartalmazza. A védjegy a szolgáltató szervezet, a MÁV INFORMATIKA Kft. tulajdona.

3.1.7. Privát kulcs birtoklás ellenőrzésének módszere

Az 1.4 pontban meghatározott összes tanúsítvány osztály és fajta szerinti kulcspár generálása a Szolgáltató hitelesítő szervezeténél történik.

Központi kulcs generálás esetén az Aláírás létrehozó és az ellenőrző adat birtoklásának és egymáshoz tartozásának ellenőrzésére nincs szükség, csupán az Aláíróhoz eljutatott Aláírás létrehozó eszköz, illetve adat átvételének igazolása szükséges. Az Aláírás létrehozó eszköz személyes átvételénél az Előfizetőnek írásban kell igazolnia az Aláírás létrehozó eszköz és a PIN kód átvételét. Az átvétel után az Előfizető teljes felelősséget kell viselnie az Aláírás létrehozó eszköz és a PIN kód biztonságos használatáért és megőrzésért.

3.1.8. Személyes azonosság hitelesítése

A személyes identitást az előfizetői osztályú, természetes személy hitelesítéséhez a HSzSz 3.1.8 pontjában meghatározott adatokat kéri a regisztráló szervezet.

Ezen adatokat a személyi igazolvány vagy az útlevél személyes bemutatásával kell hitelesíteni.

Az Előfizető írásbeli nyilatkozatot ad arra vonatkozóan, hogy:

- a Tanúsítvány kibocsátásával és fenntartásával kapcsolatos és minden egyéb járulékos költséget vállal,
- a Szolgáltató nyilvánosan közzétett szabályzataiban részletesen tárgyalt kötelezettségeit, felelősségét és jogait ismeri, s elfogadja azokat.

A Tanúsítvány kérelem nem fogadható el, amennyiben az okmányok személyhez tartozásával, eredetiségével, valódiságával vagy érvényességével kapcsolatban kétség merül fel.

A személyes identitást az előfizetői osztályú, szervezeti személy hitelesítéséhez a HSzSz 3.1.8 pontjában meghatározott adatokat kéri a regisztráló szervezet.

Ezen adatokat a következő dokumentumokkal kell hitelesíteni:

- személyi igazolvány vagy útlevél bemutatása személyesen,
- képviseleti megbízás cégszerűen aláírva,
- 30 napnál nem régebbi cégkivonat,
- aláírási címpéldány.

A Tanúsítvány kérelem nem fogadható el, amennyiben az okmányok személyhez tartozásával, eredetiségével, valódiságával vagy érvényességével kapcsolatban kétség merül fel.

3.1.9. Szervezeti identitás hitelesítése szervezeti személy tanúsítvány igénylése esetén

A szervezeti identitást az előfizetői osztályú, szervezet hitelesítéséhez a HSzSz 3.1.8 pontjában meghatározott adatokat kéri a regisztráló szervezet szervezeti személy tanúsítvány igénylése esetén.

Ezen adatokat a következő dokumentumokkal kell hitelesíteni:

- 30 napnál nem régebbi cégkivonat,
- aláírási címpéldány.

Az előfizető szervezet írásbeli nyilatkozatot ad arra vonatkozóan, hogy:

- a Tanúsítvány kibocsátásával és fenntartásával kapcsolatos és minden egyéb járulékos költséget vállal,
- a Szolgáltató nyilvánosan közzétett szabályzataiban részletesen tárgyalt kötelezettségeit, felelősségét és jogait ismeri, s elfogadja azokat.

A Tanúsítvány kérelem nem fogadható el, amennyiben az okmányok személyhez tartozásával, eredetiségével, valódiságával vagy érvényességével kapcsolatban kétség merül fel.

3.2. Érvényes tanúsítvány megújítás

Egy érvényes (nem lejárt és nem visszavont) tanúsítvány megújítására csak *tanúsítványfrissítés* esetében van lehetőség, amikor a Szolgáltató érvényes magánkulcsával az új tanúsítványban a tanúsítvány alanyának változatlan (régi) nyilvános kulcsát és változatlan egyéb adatait írja alá új érvényességi időtartamra.

Az Aláíró Tanúsítványának lejárta előtt, a HSzSz 3.2 pontjában meghatározott módon kap értesítést a Szolgáltatótól a tanúsítvány frissítés szükségességéről.

Az Aláíró értesítése után a Tanúsítvány lejártakor a Szolgáltató a Tanúsítványt frissíti, azaz az érvényességi idejét 1 évre meghosszabbítja.

(A Szolgáltató által kibocsátott előfizetői tanúsítványok érvényességi ideje 1 év.)

Előfizetői tanúsítvány frissítése akkor lehetséges, ha:

- a Tanúsítvány érvényes,
- a Tanúsítvány nem szerepel a tanúsítvány visszavonási listán, mint visszavont vagy felfüggesztett tanúsítvány,
- a kezdeti regisztráció alkalmával rögzített összes adat még érvényes, (azok is melyek a Tanúsítványban nem, csak szolgáltató belső nyilvántartásában szerepelnek),
- a Tanúsítványhoz tartozó magánkulcs nem kompromittálódott.

Ha mindezen feltételek nem teljesülnek, az Előfizetőnek új tanúsítványt kell igényelnie a kezdeti regisztráció módszerével.

Minden második évben a tanúsítvány frissítési eljárás megegyezik a „Kezdeti regisztráció" fejezetben leírtakkal. Közbenső frissítés esetén a felhasználó adatainak újbóli regisztrációjára nincs szükség. Ennek feltétele, hogy a felhasználó hitelesített elektronikus vagy írásos dokumentumban nyilatkozzon, hogy a kezdeti regisztrációkor magadott adatai nem változtak, különös tekintettel a tanúsítványban megjelenő adatokra.

Ennek érdekében a Szolgáltató:

- ellenőrzi a tanúsítvány létezését és érvényességét, valamint,
- az Aláíró azonosságának és jellemzőinek igazolására használt információ még mindig érvényes-e.

Amennyiben bármely feltétele, illetve kikötése megváltozott, közli azokat az Előfizetővel, és megegyezik vele a 4.1 pontnak megfelelően.

3.3. Érvénytelen tanúsítvány megújítás

A következő esetekben a Tanúsítványt először vissza kell vonni, majd a szükséges módosítások után új Tanúsítványt kell kibocsátani:

- *Tanúsítvány aktualizálás*, amikor a Szolgáltató érvényes magánkulcsával az új Tanúsítványban a Tanúsítvány Tulajdonosának változatlan (régi) nyilvános kulcsát és megváltozott új adatait írja alá új érvényességi időtartamra.

  Mind a Tanúsítványban foglalt, mind az abban nem foglalt adatok megváltozását az Előfizető, illetve az Aláíró személyesen, elektronikusan aláírt e-mail-ben, vagy telefonon jelentheti be.

  Személyes bejelentés esetén a szükséges azonosítás-hitelesítés elvégzése után megtörténhet a Tanúsítvány visszavonása és az új Tanúsítvány kibocsátása is.

  Telefonon vagy e-mail-en keresztül történő adatváltozás bejelentés után a Tanúsítvány visszavonáshoz és megújításhoz személyesen kell megjelenni. A bejelentéstől a személyes megjelenésig a Tanúsítványt fel kell függeszteni. Amennyiben az Előfizető vagy az Aláíró a bejelentéstől számított 30 napon belül nem jelenik meg személyesen a Tanúsítvány megújítása céljából, akkor a Tanúsítványt az Előfizető vagy az Aláíró értesítése mellett, de minden egyéb feltétel figyelembe vétele nélkül a Szolgáltató visszavonja.
- *Tanúsítvány kulcscsere*, amikor a Szolgáltató érvényes magánkulcsával az új Tanúsítványban a Tanúsítvány Aláírójának új nyilvános kulcsát és változatlan egyéb adatait írja alá új érvényességi időtartamra. A kulcscseréhez kapcsolódó Tanúsítvány megújításhoz az Előfizetőnek vagy az Aláírónak személyesen kell megjelennie.

Mind tanúsítvány aktualizálás, mind kulcscsere esetén az új Tanúsítvány igénylése csak személyesen történhet. A személy, illetve a szervezet azonosítás-hitelesítése a 3.1.8, illetve a 3.1.9 pontokban leírt eljárások szerint történhet.

Ha a Tanúsítvány visszavont vagy felfüggesztett állapotban van, illetve az érvényessége lejárt, a Tanúsítvány megújítása új Tanúsítvány igényelésével történik, a regisztrációs eljárás a 3.1.8, illetve a 3.1.9 pontok szerinti végrehajtásával.

3.4. Felfüggesztés és visszavonás kérés

Visszavonási kérés csak személyes megjelenéssel történhet. A Tanúsítvány visszavonási kérés azonosítási és hitelesítési vonatkozásai megtalálhatóak a HSzSz 4.4 fejezetében.

A Szolgáltató gondoskodik arról, hogy az előző pontban meghatározott, egy már korábban nála nyilvántartásba vett Aláírótól származó, tanúsítvány visszavonási vagy felfüggesztési kérelem teljes, pontos és kellőképpen hiteles legyen. Ennek érdekében a Szolgáltató a HSzSz 4.4 pontja szerint dokumentálja a tanúsítványok visszavonásának, felfüggesztésének eljárásait, beleértve az alábbiakat:

- ki adhat be visszavonási kérelmeket,
- hogyan lehet ezeket beadni,
- mik a visszavonási kérelmek megerősítésére vonatkozó esetleges követelmények,
- milyen okból kifolyólag függeszthető fel egy Tanúsítvány,
- mi a felfüggesztett állapot maximális időtartama.

4. A működésre vonatkozó követelmények

4.1. Tanúsítványigénylés

a. A Szolgáltatónak azt megelőzően, hogy egy Előfizetővel szerződéses kapcsolatot létesít, tájékoztatnia kell az Előfizetőt a Tanúsítvány használatával kapcsolatos kikötésekről és feltételekről a 2.6.1 pontban megadottak szerint.

b. A Szolgáltató az Aláírót is tájékoztatja kötelességeiről.

c. Az Előfizetőnek meg kell adnia egy fizikai címet, illetve más jellemzőket (lásd HSzSz 3.1 pont!), amelyek leírják, hogy az Előfizetővel hogyan lehet felvenni a kapcsolatot.

d. A Szolgáltató nyilvántartásba vesz minden, az Aláíró azonosságának igazolására használt információt, beleértve az igazoláshoz használt dokumentáció regisztrációs számát és az annak érvényességével kapcsolatos esetleges korlátozásokat.

e. A Szolgáltató nyilvántartásba veszi az Előfizetővel aláírt megállapodást[22], beleértve az alábbiakat:

   - az Előfizető kötelezettségeivel (lásd 2.1.6) történő egyetértést,
   - hozzájárulás az alábbi szolgáltatások során felhasznált információ Szolgáltató által történő nyilvántartásba vételéhez: regisztrálás, az előfizetők eszközzel való ellátása (beleértve az Előfizetőhöz történő továbbítást is), bármely ezt követő visszavonás, illetve ezen információ harmadik félhez történő továbbítása (a Szolgáltató szolgáltatásainak leállítása esetén a HSzSz által megkövetelt feltételek szerint),
   - hogy az Előfizető megköveteli-e, az Aláíró pedig hozzájárul-e a Tanúsítvány közzétételéhez és milyen feltételek mellett,
   - annak írásbeli megerősítését, hogy a Tanúsítványban szereplő információ helyes.

f. A Szolgáltató megőrzi a d)-e) pontokban megnevezett nyilvántartásokat 10 évig, illetőleg a velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig.

[22] Az Előfizető ezen megállapodás különböző pontjaihoz a regisztráció különböző fázisai során is hozzájárulhat. Például a Tanúsítványban szereplő információ helyességére vonatkozó megállapodás a megállapodás egyéb szempontjait követően is megkötheti.

A Szolgáltató lehetővé teheti 1 évnél régebben aktív ügyfelei részére tanúsítvány frissítés esetén, hogy tanúsítványaik frissítésére vonatkozó bejelentésüket ne személyesen tegyék meg. Ebben az esetben az Előfizetőnek írásban meg kell erősítenie, hogy az adatai az előző tanúsítvány igénylés óta nem változtak meg. Ez után a rendelkezésére álló adatok alapján történik meg a tanúsítvány kibocsátás. A 4.1 pontban leírt regisztrációs űrlap kitöltésnek ekkor is meg kell történnie a Tanúsítvány átadása előtt. Ilyen egyszerűsített igénylés azonban csak egyszer adható be a Szolgáltatóhoz, a következő igénylésnél az azonosítás-hitelesítést a 3.1 pont szerint el kell végezni.

4.2. Tanúsítvány kibocsátás

A Szolgáltatónak biztonságosan fenn kell tartania az általa kibocsátott tanúsítványok hitelességét. Különösképpen:

- Előállítása után a teljes és pontos Tanúsítvány rendelkezésére áll azon Előfizető vagy Aláíró számára, akinek a Tanúsítvány kibocsátásra került.
- A Tanúsítvány kibocsátás eljárása biztonságosan kapcsolódik a megfelelő regisztrációhoz, illetve a különböző tanúsítvány megújítási eljárásokhoz.
- Az Aláíró számára a Szolgáltató által megvalósított kulcselőállítás után a Tanúsítvány kibocsátás eljárása biztonságosan kapcsolódik a Szolgáltató általi kulcspár előállításhoz.
- A Szolgáltató csak akkor bocsát ki egy új Tanúsítványt az Aláíró korábbiakban tanúsított Aláírás ellenőrző adatának felhasználásával (Tanúsítvány frissítés), ha annak kriptográfiai biztonsága még megfelelő az új Tanúsítvány tervezett élettartamára, és nincsenek arra utaló jelek, hogy az Aláíró Aláírás létrehozó adata kompromittálódott. A Szolgáltató legfeljebb egy alkalommal frissítethet egy Tanúsítványt ily módon.

A hitelesítő szervezet csak akkor fogadhatja el a tanúsítványkérelmet, ha a következő feltételek teljesülnek:

- az Aláíró benyújtotta kérelmét aregisztráló szervezetnek,
- az Aláíró azonos a kérelemben szereplő alannyal (subject),
- szervezeti személy tanúsítvány igénylés esetén az azonosított és hitelesített kapcsolattartó jogosult a kérelemben szereplő Aláíró nevében kérelmet benyújtani,
- a regisztráló szervezet bejegyezte a tanúsítványkérelmet.

A Szolgáltató a Tanúsítvány kibocsátását visszautasíthatja, amennyiben:

- a bemutatott iratok és okmányok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel,
  - a cégnyilvántartással végzett adategyeztetés a bemutatott adatoktól eltérő eredményt ad,
  - a személy szervezethez tartozása nem egyértelmű,
  - a szervezet kiléte nem állapítható meg minden kétséget kizáróan,
  - nem egyértelmű a szervezet felhatalmazása a Tanúsítvány kibocsátására.

A Tanúsítvány elkészítését és kibocsátását a regisztráció során felvett űrlap alapján végzi a hitelesítő szervezet.

A hitelesítő szervezetnek az előállított Tanúsítványt vissza kell küldenie a regisztráló szervezethez. Amennyiben a tanúsítványkérelem visszautasításra kerül ennek tényéről és okáról a regisztráló szervezet értesítést kap.

4.3. Tanúsítvány elfogadás

Lásd a HSzSz 4.3 pontjában mindkét tanúsítványtípusra és csak az **MTT**-re vonatkozó részeket.

4.4. Tanúsítvány felfüggesztés és visszavonás

A Szolgáltató a tanúsítványok érvényességének kezelésére mind tanúsítvány visszavonási, mind tanúsítvány felfüggesztési szolgáltatásokat nyújt. A Tanúsítvány visszavonása a Tanúsítvány állapotát végérvényesen érvénytelenre állítja. A Tanúsítvány felfüggesztett állapotban csak ideiglenesen lehet, az engedélyezett időtartam (lásd 4.4.8 pont) után állapotát újra érvényesre kell állítani, vagy vissza kell vonni. A felfüggesztett Tanúsítvány mindaddig, míg felfüggesztett állapotban van, ugyanúgy érvénytelenként kezelendő, mint a visszavont.

A visszavont/felfüggesztett Tanúsítványhoz tartozó magánkulcs használatát azonnal meg kell szüntetni, illetve fel kell függeszteni. A visszavont Tanúsítványhoz tartozó Aláíró létrehozó adatot a visszavonást követően azonnal meg kell semmisíteni. A

megsemmisítéséig az Aláíró létrehozó adat ugyanolyan felügyeletben részesítendő, mintha érvényes lenne.

A visszavonási/felfüggesztési kérelmek fogadását és azoknak a sikeres ellenőrzés utáni végrehajtását a Szolgáltatónak mindennap 24 órában, 99,9%-os rendelkezésre állással kell biztosítania úgy, hogy az esetenkénti a visszavonási/felfüggesztési kezelés kiesése nem lehet több, mint 3 óra.

4.4.1. Visszavonáshoz vezető körülmények

A Szolgáltató HSzSz 4.4.1 pontja határozza meg, hogy milyen körülmények között lehet, illetve kell visszavonási kérelmet benyújtani.

4.4.2. Visszavonás kérelmezése

A Szolgáltató HSzSz 4.4.2 pontja határozza meg, hogy ki és milyen módon nyújthat be visszavonási kérelmet.

4.4.3. Visszavonási eljárás

A Szolgáltató HSzSz-e dokumentálja a tanúsítványok visszavonásának eljárásait, beleértve az alábbiakat:

- hogyan lehet ezeket beadni,
- a visszavonási kérelmek megerősítésére vonatkozó esetleges követelmények.

A Szolgáltató a tanúsítványok visszavonásra vonatkozó kérelmeket fogadásuk után haladéktalanul feldolgozza.

A visszavonásra vonatkozó kérelmeket hitelesíteni kell, a Szolgáltató ellenőrzi, hogy hiteles forrásból származnak-e. Az ilyen kérelmeket meg kell erősíteni azokban az esetekben, amelyekben ezt a Szolgáltató HSzSz-e megköveteli.

A Szolgáltató tájékoztatja a visszavont Tanúsítvány tulajdonosát, és ahol ez alkalmazható az Előfizetőt, a Tanúsítvány állapotának megváltozásáról.

A Szolgáltató nem állítja vissza érvényesre a már egyszer véglegesen visszavonásra (azaz nem felfüggesztésre) került tanúsítványokat.

4.4.4. Visszavonási kérelemre vonatkozó türelmi idő

A visszavonási kérelem esetén a bejelentési kötelezettség azonnali, a Szolgáltató a kérelmet soron kívül végrehajtja annak elfogadása után. A legnagyobb késedelem a visszavonási kérelem fogadása, illetve az összes érintett fél rendelkezésére álló információ visszavonási állapotának megváltoztatása között: 24 óra.

A Tanúsítvány érvényességének lejárata előtti - bármely okból történő - visszavonása esetén a Tanúsítványt a továbbiakban joghatályosan nem lehet felhasználni.

A Szolgáltatót és az Előfizetőt érintő felelősségi szabályokat a HSzSz 4.4.4 pontja határozza meg.

Az Érintett fél, amennyiben a tudomására jut adott Tanúsítvány érvénytelenségére utaló információ, nem hagyatkozhat kizárólag a Címtárban megjelenő érvényességi adatokra.

4.4.5. Felfüggesztéshez vezető körülmények

A Szolgáltató megerősítést igénylő visszavonási kérelem esetén a Tanúsítvány visszavonási állapotát „felfüggesztett”-re állítja, amíg a visszavonás megerősítésre nem kerül.

A Szolgáltató HSzSz-e határozza meg, hogy a tanúsítványok milyen okból kifolyólag függeszthetők fel.

4.4.6. Felfüggesztés kérelmezése

A Szolgáltató HSzSz 4.4.6 pontja határozza meg, hogy kik és milyen módon kérelmezhetik a tanúsítványok felfüggesztését.

4.4.7. Felfüggesztési eljárás

A Szolgáltató HSzSz 4.4.7 pontja határozza meg a felfüggesztési kérelemre vonatkozó pontos eljárást.

A Szolgáltató a tanúsítványok felfüggesztésére vonatkozó kérelmeket fogadásuk után haladéktalanul feldolgozza.

A Szolgáltató tájékoztatja a felfüggesztett Tanúsítvány tulajdonosát, és ahol ez alkalmazható az Előfizetőt, a Tanúsítvány állapotának megváltozásáról.

4.4.8. Felfüggesztett állapotra vonatkozó korlátozások

A Szolgáltató gondoskodik arról, hogy egy Tanúsítvány ne legyen hosszabb ideig felfüggesztve, mint amennyi állapotának megerősítéséhez szükséges.

4.4.9. CRL kibocsátás gyakorisága

A Szolgáltató a visszavonási állapot információt Tanúsítvány visszavonási listák egy Címtáron keresztül történő nyilvánosságra hozatalán keresztül nyújtja.

A Szolgáltató a Tanúsítvány visszavonási listákat legalább *7* óránként közzé teszi.

4.4.10. CRL ellenőrzési követelmények

A Szolgáltató meg kell védenie a Tanúsítvány visszavonási lista sértetlenségét és hitelességét.

4.4.11. On-line visszavonási státusz-szolgáltatás

A Szolgáltató on-line visszavonási állapot-szolgáltatást nem üzemeltet.

4.4.12. On-line visszavonás ellenőrzési követelmények

A Szolgáltató on-line visszavonási állapot-szolgáltatást nem üzemeltet.

4.4.13. Visszavonási állapot közlés más formái

A Szolgáltató nem alkalmaz a Tanúsítvány visszavonási listától különböző visszavonási állapot közlő eljárást.

A Tanúsítványt igénybe vevő érintett feleknek ugyanakkor, minden hagyományosan alkalmazott, és ésszerűen elvárható módszert igénybe kell venniük az általuk Tanúsítvány segítségével ellenőrzött műveletek biztonsága érdekében. Amennyiben módjuk van az aláírás és Tanúsítvány érvényességének más forrásból való ellenőrzésére, akkor azt a Tanúsítvány állapotától függetlenül is meg kell tenniük.

Amennyiben Érintett fél más forrásból tudomást szerezhet, vagy ésszerű és elvárható gondossággal más forrásból megbizonyosodhat a tanúsítvánnyal igazolt művelet

érvényességéről, akkor ezeket a lépéseket a Tanúsítvány állapotától függetlenül is meg kell tennie. Szolgáltató ilyen esetekben nem felelős a bekövetkező károkért.

4.4.14. Visszavonási állapot közlés más formáinak ellenőrzési követelményei

Szolgáltató nem alkalmaz a Tanúsítvány visszavonási listától különböző visszavonási állapot közlő eljárást.

4.4.15. Magánkulcs kompromittálódás speciális követelményei

Az Aláírás létrehozó adat kompromittálódása, vagy vélelmezett kompromittálódása esetén a Tanúsítvány visszavonásáról azonnal intézkedni kell. Alapos gyanú esetén az Aláírás létrehozó adat használatát azonnal fel kell függeszteni.

Kompromittálódott magánkulcs tovább nem használható. A kompromittálódott Aláírás létrehozó adat a megsemmisítéséig ugyanolyan felügyeletben részesítendő, mint egy érvényes Aláírás létrehozó adat.

Az Előfizetőnek kötelessége a kompromittálódott Aláírás létrehozó adat által esetlegesen érintett felek értesítése, és minden intézkedés megtétele az esetleges károk megelőzése és enyhítése érdekében.

4.5. Biztonsági audit eljárások

A Szolgáltató hitelesítés támogató informatikai rendszerének biztonsági naplózását és annak auditálását a Biztonsági Szabályzat szabályozza részletesen.

A jelen dokumentumban leírt tanúsítványtípus csak regisztrációs információk, a Szolgáltató kulcsgondozási és tanúsítványgondozási eseményeire vonatkozó információk naplózásának alábbi általános jellegzetességeit adja meg:

- A Szolgáltató a környezetére, kulcs- és Tanúsítvány gondozására vonatkozó események pontos időpontját is rögzíti[23].

[23] A HSzSz ismerteti az események időzítéséhez használt óra pontosságát, és azt, hogy ez a pontosság hogyan van biztosítva.

- A Szolgáltató biztosítja személyzete felelősségre vonhatóságát tevékenységéért, többek között az eseménynapló megőrzésén és védelmén keresztül (lásd 4.5.1, 4.5.4, 4.5.5).

4.5.1. Naplózott esemény típusok

A Szolgáltató általános tevékenységével kapcsolatosan:

- A naplózandó speciális eseményeket és adatokat a Szolgáltató HSzSz-ében dokumentálja.

A regisztrációval kapcsolatosan:

- A Szolgáltató gondoskodik arról, hogy naplózásra kerüljön valamennyi regisztrációval kapcsolatos esemény, beleértve a Tanúsítvány megújítására (Tanúsítványfrissítésre, Tanúsítvány aktualizálására és Kulcscserére) vonatkozó kérelmeket is.

A Tanúsítvány előállítással kapcsolatosan:

- A Szolgáltató naplózza a szolgáltatói kulcsok életciklusával kapcsolatos összes eseményt.
- A Szolgáltató naplózza a tanúsítványok életciklusával kapcsolatos összes eseményt.

Az aláírók Aláírás létrehozó eszközzel való ellátásával kapcsolatosan[24]:

- A Szolgáltató naplóz minden általa gondozott kulcs életciklusával kapcsolatos eseményt.
- a Szolgáltató naplózza az Aláírás létrehozó eszközök készítésével kapcsolatos valamennyi eseményt.

A visszavonás kezeléssel kapcsolatosan:

- A Szolgáltató gondoskodik a visszavonással kapcsolatos összes kérés, valamint az ezek eredményét képező összes tevékenység naplózásáról.

A hitelesítés támogató informatikai rendszer operációs rendszere szintjén a Biztonság politikában és a Biztonsági Szabályzatban meghatározott események kerülnek naplózásra.

4.5.2. Napló adatok feldolgozásának gyakorisága

[24] Az „aláírás létrehozó eszközön az aláírás létrehozó adat elhelyezése” szolgáltatás keretén belül.

A napló állományok feldolgozásának gyakoriságát a Szolgáltató HSzSz 4.5.2 pontja határozza meg.

4.5.3. Napló adatok tárolási ideje

A napló adatok tárolási idejét a Szolgáltató HSzSz 4.5.3 pontja határozza meg.

4.5.4. Napló adatok védelme

A Szolgáltató az eseményeket oly módon naplózza, ami nem törölhető, illetve nem tehető tönkre azon időtartam alatt, amíg azokat meg kell őrizni.

A Szolgáltató biztosítja a tanúsítványok és kulcsok gondozására[25] vonatkozó napló rekordok bizalmasságát és sértetlenségét.

4.5.5. Napló adatok mentési eljárásai

A napló állomány mentési eljárásait a Szolgáltató HSzSz 4.5.5 pontja határozza meg..

4.5.6. A napló gyűjtési rendszere

A napló gyűjtési rendszerét a Szolgáltató HSzSz 4.5.6 pontja határozza meg.

4.5.7. Rendkívüli eseményekről történő értesítés

A hitelesítés szolgáltatást leállását eredményező súlyos üzemzavari vagy katasztrófa, illetve a szolgáltatói Aláírás létrehozó és aktiváló adatait kompromittáló események esetén haladéktalanul értesítésre kerülnek:

- a Szolgáltatónak az Üzletmenet-folytonossági Tervben meghatározott felső vezetői,
- a Válság Stáb vezetője és tagjai,
- szükség esetén az ilyen események kezelésére szerződéssel lekötött szerviz cégeknek, az Üzletmenet-folytonossági Tervben megnevezett munkatársai.

[25] Minden a tanúsítványokkal és kulcsokkal kapcsolatos művelet ide értendő. A hardverek (pl. UPS) és más biztonsági berendezések (pl. tűzfalak) valamint az operációs rendszerek és egyéb szoftverek (pl. vírusvédelmi szoftverek) naplóállományai külön kategóriát jelentenek.

A Szolgáltató nem értesíti a naplóbejegyzéseket kiváltó alanyokat, szükség esetén azonban bevonhatja őket az esemény kivizsgálásába.

4.5.8. Sebezhetőség kiértékelése

A sebezhetőség felmérésére végzett tevékenységeket a Szolgáltató HSzSz 4.5.8 pontja határozza meg.

Az aktuális sebezhetőségi szintek biztonsági ellenőrzése és kiértékelése a 6.5.2 pont szerint történik.

4.6. Adatarchiválás

A Szolgáltatónak gondoskodnia kell arról, hogy a Tanúsítványra vonatkozó minden lényeges információ megfelelő ideig rögzítésre kerüljön, különösen jogi eljárásokhoz bizonyíték nyújtása érdekében[26].

4.6.1. A tárolt események típusai

A Szolgáltató gondoskodik arról, hogy rögzítésre kerüljön az összes regisztrációs információ, beleértve az alábbiakat is:

- az Igénylő által a regisztráció támogatása céljából benyújtott dokumentum(ok) típusa,
- az azonosító dokumentumok egyedi azonosító adatai (például az Igénylő jogosítvány száma),
- az Igénylő és azonosító dokumentumok (beleértve az aláírt, az Előfizetővel kötött megállapodást másolatainak tárolási helyszíne,
- az Előfizetővel kötött megállapodás esetleges egyedi választásai (például a Tanúsítvány közzétételéhez történő hozzájárulás),
- a kérelmet elfogadó regisztrációs felügyelő (RO) azonosítója,
- a fogadó hitelesítő szervezet és/vagy a küldő regisztráló szervezet neve, amennyiben ez értelmezhető.

[26] A tanúsítványokra vonatkozó rekordok regisztrációs információt és a Szolgáltató környezeti, kulcs- és tanúsítvány gondozási eseményeire vonatkozó fontos információt tartalmaznak.

A tanúsítványokra vonatkozó valamennyi naplóbejegyzés archiválásra kerül (lásd 4.5.1 pontot).

Azon eseményeket, mely a fent említett naplóbejegyzéseken túl kerülnek archiválásra (a biztonságos környezet fenntartásának és utólagos ellenőrizhetősége és bizonyíthatósága céljából), a Szolgáltató HSzSz-e határozza meg.

4.6.2. Az archívum megőrzési időtartama

A Szolgáltató a 4.1 d) és e) pontjában megnevezett nyilvántartásokat a 4.1 f. pontban meghatározott ideig megőrzi, illetve jogi eljárásban a tanúsítványokon keresztül történő bizonyításhoz szükséges ideig.

A Szolgáltató a tanúsítványokra vonatkozó napló adatokat (lásd 4.5.1 pontot) a 16/2001. (IX.1.) MeHVM rendelettel összhangban a keletkezésüktől számított 10 évig kell megőrizni.

A biztonságos környezet fenntartásának utólagos ellenőrizhetősége és bizonyíthatósága érdekében archivált egyéb naplóbejegyzések megőrzési időtartamát a Szolgáltató HSzSz 4.6.2 pontja határozza meg.

4.6.3. Az archívum védelme

A Szolgáltató fenntartja a tanúsítványokra vonatkozó aktuális és archivált adatok bizalmasságát és sértetlenségét.

A Szolgáltató a tanúsítványokra vonatkozó naplóadatokat teljes körűen és a bizalmasságot garantáló módon archiválja a szolgáltatás szabályzatban leírt üzleti gyakorlatnak megfelelően.

A Szolgáltató a fontos bejegyzéseket megvédi az elveszéstől, tönkretételtől és hamisítástól.

A Szolgáltató megfelelő műszaki és szervezeti intézkedéseket hoz a személyes adatok felhatalmazás nélküli, illetve törvénytelen feldolgozása ellen, valamint a személyes adatok véletlen elveszése, megsemmisülése, illetve károsodása ellen.

Az archívumba történő hagyományos vagy elektronikus adattovábbítás csak biztonságos megoldással történhet.

4.6.4. Az archívum mentési folyamatai

Az archívum mentési folyamatait a Szolgáltató HSzSz 4.6.4 pontja határozza meg.

4.6.5. A rekordok időbélyegzésére vonatkozó követelmények

Az archívum időbélyegzésére vonatkozó követelményeit és gyakorlatát a Szolgáltató HSzSz 4.6.5 pontja határozza meg.

4.6.6. Az archívum gyűjtési rendszere

Az archívum gyűjtési rendszerét a Szolgáltató HSzSz 4.6.6 pontja határozza meg.

4.6.7. Archív információ hozzáférését és ellenőrzését végző eljárások

A Szolgáltató az archívumhoz regisztrálószervezetén keresztül biztosít hozzáférést. A hozzáférés az Aláírónak és az Előfizetőnek a rá vonatkozó adatokhoz lehetséges, más feleknek a 2.8.4, 2.8.5 és 2.8.6 pontok szerint. A Szolgáltató a jogosultságot minden esetben ellenőrzi, és azt naplózza.

4.7. Kulcs csere

A kulcs csere feltételeit és módját a Szolgáltató HSzSz 4.7 pontja határozza meg

4.8. Katasztrófa elhárítás

A Szolgáltató gondoskodik arról, hogy katasztrófa esetén, beleértve a saját aláírás létrehozó magánkulcsának kompromittálódását, illetve kritikus szoftver/hardver komponenseinek meghibásodását is, az üzemeltetés amint csak lehetséges helyreálljon.

4.8.1. Hardver, szoftver, vagy adatsérülés esete

A Szolgáltató Üzletmenet-folytonossági Terve a kritikus szoftver/hardver komponensek sérülésével, mint katasztrófa helyzettel foglalkozik. Ilyen esetekben a tervezett eljárásokat életbe lépteti annak érdekében, hogy az üzemeltetés, amint csak lehetséges, helyreálljon.

A Szolgáltató minimalizálja a biztonsági események és hibás működések által okozott kárt, eseményjelentés és válaszadás eljárások használatán keresztül.

A Szolgáltató időben és összehangoltan fellép annak érdekében, hogy gyorsan válaszolni tudjon a váratlan eseményekre, és korlátozza a biztonság megsértésének hatásait. Ennek érdekében valamennyi eseményt jelenteni kell az esemény bekövetkezte után, amint az lehetséges.

4.8.2. Egy szolgáltatói egység nyilvános kulcsának visszavonása

Egy szolgáltatói kulcs visszavonása esetén a Szolgáltató az alábbiakat vállalja:

- a visszavonásról tájékoztatja az összes Előfizetőt és Érintett felet,
- jelzi, hogy az adott szolgáltatói kulcs felhasználásával kiadott tanúsítványok vagy visszavonási állapot információ már nem érvényes(ek).

A Szolgáltató a szolgáltatói kulcs visszavonását előidéző okok megszüntetése érdekében helyreállítja a biztonságos környezetet, valamint az előfizetők számára új nyilvános kulcsot biztosít új Tanúsítvány kiadásával.

4.8.3. Egy szolgáltatói egység kulcsának kompromittálódása

Egy szolgáltatói kulcs kompromittálódása esetén a Szolgáltató az alábbiakat vállalja:

- a kompromittálódásról tájékoztatja az összes Előfizetőt és Érintett felet,
- jelzi, hogy az adott szolgáltatói kulcs felhasználásával kiadott tanúsítványok vagy visszavonási állapot információ már nem érvényes(ek).

A Szolgáltató a szolgáltatói kulcs kompromittálódását előidéző okok megszüntetése érdekében helyreállítja a biztonságos környezetet, valamint az előfizetők számára új Aláírás ellenőrző adatot biztosít új Tanúsítvány kiadásával.

4.8.4. Biztonsági képesség egy természeti vagy más egyéb katasztrófát követően

Természeti vagy más egyéb katasztrófát követően a Szolgáltató életbe lépteti Üzletmenet-folytonossági Terve által megtervezett eljárásokat annak érdekében, hogy az üzemeltetés helyreálljon a Üzletmenet-folytonossági Tervben megjelölt időn belül.

Egy katasztrófát követően a Szolgáltató (ha ez ésszerű) lépéseket tesz a katasztrófa ismételt bekövetkezésének megakadályozására.

4.8.5. Üzletmenet-folytonossági Terv

A Szolgáltatónak rendelkeznie kell Üzletmenet-folytonossági Tervvel. Ez a dokumentum biztonsági okokból nem nyilvános.

4.9. Hitelesítés szolgáltató tevékenység megszüntetése

A Szolgáltató gondoskodik a szolgáltatásainak megszüntetéséből/ szüneteltetéséből fakadó, az előfizetőket és az érintett feleket érintő potenciális zavar minimalizálásáról. Különösképpen gondoskodik a jogi eljárásokhoz szükséges Tanúsítvány nyilvántartások fenntartásáról.

Ennek érdekében – a Szolgáltató általános tevékenységével kapcsolatosan – mielőtt egy Szolgáltató leállítja szolgáltatásait, végrehajtja az alábbi eljárásokat:

- tájékoztatja az összes Előfizetőt és Érintett felet[27], a minősített HSzSz 4.9 pontja szerint,
- megszünteti a tanúsítványok kibocsátási folyamatában a nevében eljáró alvállalkozások összes felhatalmazását,
- megteszi a szükséges lépéseket, hogy a regisztrációs információ (lásd 3.1) és az eseménynapló archívumok (lásd 4.6) fenntartására vonatkozó kötelezettségeket átruházza arra az időtartamra, amelyről az előfizetőket és az érintett feleket tájékoztatta (lásd 2.6),
- magánkulcsait megsemmisíti, illetve visszavonja a használatból a 6.2.9 alatt meghatározottak szerint.

A Szolgáltató szerződést köt a fenti követelmények teljesítésével kapcsolatos költségek fedezésére, arra az esetre, ha csődbe menne, vagy más okból kifolyólag nem lenne képes a költségeket saját maga állni.

[27] A Szolgáltatónak nem kell előzetes kapcsolatban állnia az érintett felekkel.

A Szolgáltató HSzSz-e tartalmazza a szolgáltatás leállítása esetén alkalmazott konkrét eljárásokat, melyek magukban foglalják az alábbiakat:

- az érintettek értesítését,
- saját kötelezettségeinek más felekre történő átruházását,
- a már kibocsátott, de még le nem járt tanúsítványok visszavonási állapotának a kezelését.

5. Fizikai, eljárásrendi, és humán biztonsági szabályozások

A Szolgáltató gondoskodik arról, hogy kellő, az elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések, illetve az ezeket érvényre juttató adminisztratív és irányítási eljárások kerüljenek alkalmazásra. Ezen belül:

- A Szolgáltató kockázat elemzést végzett üzleti kockázatainak felmérése, valamint a szükséges biztonsági követelmények és működési eljárások meghatározása érdekében.
- A Szolgáltató felelősséget vállal minden elektronikus aláírással kapcsolatos szolgáltatásért, még akkor is, ha bizonyos funkciókat alvállalkozóknak ad ki. A Szolgáltató egyértelműen meghatározza a harmadik felek felelősségét, és megfelelő konstrukciók biztosítják azt, hogy a harmadik felek a Szolgáltató által megkövetelt összes ellenőrzés végrehajtására legyenek szorítva. A Szolgáltató felelősséget vállal valamennyi fél fentiekre vonatkozó gyakorlatának nyilvánosságra hozására.
- A Szolgáltató vezetősége (mely felelős a Szolgáltató informatikai biztonság politikájának meghatározásáért, és e politika által érintett valamennyi alkalmazott részére történő közzétételért) az információ biztonságára vonatkozó útmutatót hagyott jóvá és adott ki.
- A Szolgáltató a szervezetén belüli biztonságkezeléshez szükséges informatika biztonsági infrastruktúrát folyamatosan fenntartja. A biztonság szintjére hatást gyakorló bárminemű változtatást a Szolgáltató vezetőségének kell jóváhagynia[28].
- A Szolgáltató a Biztonsági Szabályzatában dokumentálta, majd megvalósította és folyamatosan fenntartja a hitelesítési szolgáltatásokat nyújtó eszközök, rendszerek és informatikai értékek biztonsági ellenőrzéseit és üzemeltetési eljárásait[29].

[28] Az informatika biztonság kezelésével kapcsolatban útmutatásként lásd a MeH 12. ajánlást és az ISO/IEC 17799-et.

[29] Ajánlott, hogy a Biztonsági Szabályzat azonosítsa a nyújtott szolgáltatásokkal kapcsolatos valamennyi fontos célt és potenciális veszélyt, valamint az ezen veszélyek hatásainak elkerülése, illetve korlátozása érdekében szükséges védelmi intézkedéseket. Ajánlott leírnia az arra vonatkozó szabályokat, irányelveket és eljárásokat, hogy a meghatározott szolgáltatásokat és az ezekkel kapcsolatos biztonsági garanciákat hogyan biztosítják.

- A Szolgáltató gondoskodik az informatika biztonság fenntartásáról azokban az esetekben is, amikor az elektronikus aláírással kapcsolatos szolgáltatások egyes funkcióira vonatkozó felelősség más szervezethez, illetve egységhez lettek kiadva.
- A Szolgáltató biztonsági műveleteiért a végső felelősség a felső vezetőségéé. Ezen biztonsági műveletek közé az alábbiak tartoznak:
  - üzemeltetési eljárások és felelősségek
  - biztonsági rendszerek tervezése és elfogadása
  - káros szoftver elleni védelem
  - erőforrás gazdálkodás
  - hálózat menedzselés
  - a biztonsági napló aktív felügyelete, eseményelemzések és nyomkövetések
  - adathordozó eszköz kezelése és biztonsága
  - adat és szoftver csere

  E felelősségeket a Szolgáltató biztonsági műveletei kezelik, és azokat a 16/2001. (IX.1.) MeHVM rendelet 16.§-18.§-nak megfelelő, megbízható és szakértő üzemeltető személyzetnek kell végrehajtania.

A Szolgáltató gondoskodik arról, hogy eszközei és információi megfelelő szintű védelemben részesüljenek. Szolgáltató valamennyi informatikai értékéről leltárt vezet, ezek védelmi követelményeit osztályokba sorolja és minősíti, az elvégzett kockázat elemzéssel összhangban.

5.1. Fizikai biztonsági szabályozások[30]

5.1.1. A telephely elhelyezése és szerkezeti felépítése

A Szolgáltató általános tevékenységével kapcsolatosan:

- A Szolgáltató biztosítja az értékek elvesztésének, sérülésének, és kompromittálódásának, valamint a működési tevékenységek megzavarásának elkerülését.
- A Szolgáltató óvintézkedéseket valósít meg az információ és az információ feldolgozó berendezések kompromittálódásának, illetve ellopásának elkerülése érdekében.

Tanúsítvány előállítással, aláírók aláíró eszközzel való ellátással, visszavonás kezeléssel kapcsolatosan:

- A Szolgáltató egy egyértelműen meghatározott biztonsági körlet létrehozásával fizikai védelmet biztosít az alábbi szolgáltatások számára:
  - tanúsítvány előállítás,
  - az aláírók aláíró eszközzel való ellátása,
  - visszavonás kezelés.

  Bármely más szervezettel megosztott rész e körleten kívül esik.
- A Szolgáltató óvintézkedéseket valósít meg a fizikai és környezetbiztonsági rendszer erőforrások, illetve a működésük támogatására használt berendezések megvédése érdekében. A Szolgáltató
  - tanúsítvány előállítás,

[30] Az alábbiakban megadjuk a fizikai óvintézkedések kidolgozásánál hasznosítható, vonatkozó MSZ, honosított EN szabványok és ajánlások jegyzékét:
- 253/1997. (XII.20.) Korm. rendelet, az Országos Településrendezési és Építési Követelményekről (OTÉK)
- 35/1996. (XII.29) BM rendelet az Országos Tűzvédelmi Szabályzat (OTSZ) kiadásáról, a 9/2000. (II.16.) BM rendelettel módosítva
- az MSZ 172 szabvány csoport a villamos érintésvédelemről
- az MSZ 274 szabvány csoport a Villámvédelemről
- az MSZ 1600 szabvány csoport, érintésvédelmi biztonsági szabályzatok
- az MSZ 2365 szabvány csoport, erősáramú berendezések létesítéséről
- az MSZ 4851 szabvány csoport, az érintésvédelmi vizsgálati módszerekről
- az MSZ 6240 szabvány csoport, a belsőtéri mesterséges világításról
- az MSZ EN 50081 szabvány csoport az EMC-ről
- az MSZ IEC 1312 szabvány csoport az elektromágneses villámimpulzus elleni védelemről

- az aláírók aláíró eszközzel való ellátása,
- visszavonás kezelés

szolgáltatásainak fizikai- és környezetbiztonsági programjai foglalkoznak a fizikai hozzáférés szabályozásával, a természeti katasztrófa elleni védelemmel, a villámvédelem és tűzbiztonság tényezőivel, a támogató eszközök (ezen belül az áram és klíma berendezések) meghibásodásával, az építmény összeomlásával, vízvezeték szivárgással, talajvíz elleni védelemmel, lopás, betörés és behatolás elleni védelemmel, katasztrófa utáni helyreállítással, stb.[31]

♦ A Szolgáltató óvintézkedéseket valósít meg annak megakadályozása érdekében, hogy az elektronikus aláírással kapcsolatos szolgáltatáshoz szükséges berendezést, információt, adathordozót vagy szoftvert jogosulatlanul elvigyék a helyszínről[32].

5.1.2. Fizikai hozzáférés

A Szolgáltató a

♦ tanúsítvány előállítás,
♦ az aláírók aláíró eszközzel való ellátása,
♦ visszavonás kezelés

szolgáltatásokkal kapcsolatos eszközökhöz történő fizikai hozzáférést megfelelően felhatalmazott egyénekre korlátozza.

A Szolgáltató a

♦ tanúsítvány előállítás,
♦ az aláírók aláíró eszközzel való ellátása,

szolgáltatásokkal kapcsolatos eszközöket olyan környezetben működteti, amely fizikailag megvédi a szolgáltatásokat attól, hogy a rendszerekhez, illetve adatokhoz történő jogosulatlan hozzáférésen keresztül kompromittálódjanak.

Részletesen lásd HSzSz 5.1.1 pontját.

[31] A fizikai és környezeti biztonsággal kapcsolatban útmutatóként lásd a MeH 12. ajánlását és az ISO/IEC 17799 dokumentumot.
[32] A biztonsági körletben egyéb funkciók is támogathatók, a hozzáférések jogosult személyzetre való korlátozás biztosításával.

5.1.3. Áramellátás, légkondicionálás

Lásd HSzSz 5.1.1 pontját.

5.1.4. Beázás és elárasztódás veszélyeztetettsége

Lásd HSzSz 5.1.1 pontját.

5.1.5. Tűzmegelőzés és tűzvédelem

Lásd HSzSz 5.1.1 pontját.

5.1.6. Adathordozók tárolása

A Szolgáltató az adathordozó eszközöket biztonságosan kezeli a sérülés, ellopás és jogosulatlan hozzáférés elleni védelem érdekében.

A Szolgáltató az összes adathordozó eszközt biztonságosan kezeli az adat-minősítési rendszer követelményeinek megfelelően (lásd a HSzSz 5.1.1 pontját.).

5.1.7. Selejt kezelése, megsemmisítése

A Szolgáltató az érzékeny adatokat tartalmazó adathordozó eszköztől biztonságosan válik meg, amennyiben azokra már nincs szükség.

5.1.8. Fizikailag elkülönítetten őrzött mentési példányok

Lásd a HSzSz 4.5 és 4.6 pontjait.

5.2. Eljárásrendi szabályozások

A Szolgáltató gondoskodik arról, hogy rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltessék.

A Szolgáltató személyzete olyan adminisztratív és kezelési eljárásokat és folyamatokat végez, amely szinkronban van a Szolgáltató Biztonsági Szabályzatának eljárásaival.

5.2.1. Bizalmi munkakörök

A Szolgáltató a HSzSz 5.2 pont egyértelműen azonosítja azokat a biztonsági munkaköröket, amelyektől a Szolgáltató működésének biztonsága függ. Ezeket a biztonsági munkaköröket és felelősségeket munka leírásokban dokumentálja.

A bizalmi munkakörök közé az alábbi munkakörök tartoznak, egyúttal az alábbi felelősségekkel járnak:

- Biztonsági tisztviselők (infrastruktúra szintű biztonsági adminisztrátorok és PKI szintű Security Officer-ek (SO): általánosságban felelősek a biztonsági szabályzatok végrehajtásáért. A biztonsági tisztviselő hagyja jóvá a tanúsítványok előállítását, visszavonását és felfüggesztését[33] is.
- Rendszer adminisztrátorok: fel vannak hatalmazva arra, hogy a Szolgáltató megbízható rendszereit telepítsék, konfigurálják és karbantartsák a:
  - tanúsítvány előállítás,
  - az aláírók aláíró eszközzel való ellátása,
  - visszavonás kezelés

  céljából.
- Rendszer operátorok: felelősek a Szolgáltató megbízható rendszereinek folyamatos üzemeltetéséért. Fel vannak hatalmazva a rendszermentések és helyreállítások végrehajtására.
- Rendszer auditorok: fel vannak hatalmazva a Szolgáltató megbízható rendszerei archívumainak és biztonsági naplóinak megtekintésére és karbantartására.
- A bizalmi munkakörök közötti személyi átfedésekre az alábbi korlátozások vonatkoznak:
  - a rendszer adminisztrátor nem kaphat biztonsági tisztviselői vagy rendszervizsgálói jogokat,
  - a biztonsági tisztviselő nem kaphat rendszervizsgálói jogokat.
- A bizalmi munkakörökbe a Szolgáltató biztonságért felelős felső vezetése nevezi ki a munkatársakat.

[33] Megjegyzés: A biztonsági tisztviselő munkaköre megosztható. Pl. a regisztrációs biztonsági tisztviselő munkakör a biztonsági tisztviselő munkakörének egy olyan rész-munkaköre, melyben dolgozó csak a tanúsítvány előállítás, visszavonás és felfüggesztés jóváhagyására jogosult (SO).

- Valamennyi olyan bizalmi és adminisztratív munkakörre, amely hatást gyakorol a hitelesítési szolgáltatások nyújtására, előzetesen kidolgozott eljárások kerülnek végrehajtásra.

5.2.2. Az egyes feladatokhoz szükséges személyzeti létszámok

- A Szolgáltató (ideiglenes és állandó) munkatársainak munkaleírásai támogatják a feladatok szétválasztása és a legkisebb meghatalmazás szempontjait. A munkaleírások többek között meghatározzák az egyes feladatokhoz szükséges létszámot is.
- Csak bizalmi munkakört betöltő személyzet végezheti legalább kettős ellenőrzés mellett az alábbi funkciókat:
  - a Szolgáltató saját (szolgáltatói) kulcsának előállítása,
  - a Szolgáltató aláíró kulcsainak kriptográfiai hardverben történő installálása, aktivizálása,
  - a Szolgáltató magán aláíró kulcsának másolása, letárolása, visszaállítása,
  - a Szolgáltató magán aláíró kulcsának megsemmisítése.

  A fenti funkciók végrehajtására felhatalmazott személyzet köre a Szolgáltató HSzSz-ének megfelelve, a lehető legkisebbre van korlátozva.

5.2.3. Az egyes munkakörökben elvárt azonosítás és hitelesítés

A Szolgáltató személyzete csak sikeres azonosítás és hitelesítés után használhatja a kulcs- és tanúsítvány gondozással kapcsolatos kritikus alkalmazásokat.

5.3. Humán szabályozások

A Szolgáltató gondoskodik arról, hogy személyzeti, illetve a munkatársak alkalmazására vonatkozó gyakorlatai fokozzák és támogassák a Szolgáltató működésének megbízhatóságát. Különösképpen:

- A Szolgáltató kellő számú, az elektronikus aláírással kapcsolatos szolgáltatások nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai ismerettel és tapasztalattal rendelkező személyzetet alkalmaz.

- A Szolgáltató valamennyi bizalmi munkakört betöltő munkatársa független minden olyan ütköző érdektől, ami hátrányosan érinthetné a Szolgáltató tevékenységeinek semlegességét.
- A Szolgáltató (ideiglenes és állandó) munkatársainak a feladatok szétválasztása és a legkisebb meghatalmazás szempontjai szerint meghatározott munkaleírásokkal rendelkeznek. A munkaleírások meghatározzák a beosztás érzékenységét, a feladatok és a hozzáférési szintek, a háttér-ellenőrzés, az alkalmazott képzettség és tudatosság alapján. Ahol erre szükség van, megkülönböztetik az általános funkciókat és a Szolgáltató specifikus funkciókat. A munkaleírások meghatározzák az egyes feladatokhoz szükséges létszámot is. A munkaleírások tartalmazzák a szakismeretre és a tapasztalatra vonatkozó követelményeket is.

5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

A Szolgáltató olyan személyzetet alkalmaz, amely rendelkezik a kínált szolgáltatáshoz szükséges szakértői tudással, tapasztalattal és minősítésekkel.

A Szolgáltató kellő számú, a hitelesítési szolgáltatások nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai ismerettel és tapasztalattal rendelkező személyzetet alkalmaz.

A vezető személyzet tapasztalattal rendelkezik az elektronikus aláírási technológia terén, ismeri a biztonsági felelősséggel tartozó munkatársakra vonatkozó biztonsági eljárásokat, valamint gyakorlattal rendelkezik az informatika biztonság és a kockázat elemzés területein.

5.3.2. Biztonsági háttér ellenőrzésekre vonatkozó eljárások

A Szolgáltató nem nevez ki bizalmi munkakörbe, illetve a vezetőségbe olyan személyt, aki bűncselekményért, illetve más olyan vétségért el lett ítélve, amely beosztást illető alkalmasságát befolyásolja. A munkatársak nem férhetnek biztonsági funkciókhoz a szükséges, személyükre és alkalmasságukra vonatkozó ellenőrzések végrehajtása előtt.

5.3.3. Kiképzési követelmények

A Szolgáltató személyzete rendelkezik a kínált szolgáltatásokhoz szükséges szakértői tudással, tapasztalattal és minősítésekkel.

5.3.4. Továbbképzési gyakoriságok és követelmények

Lásd a HSzSz 5.3.4 pontját.

5.3.5. Munkabeosztás körforgásának gyakorisága és sorrendje

Lásd a HSzSz 5.3.5 pontját.

5.3.6. A felhatalmazás nélküli tevékenységek büntető következményei

Lásd a HSzSz 5.3.6 pontját.

5.3.7. A szerződéses alkalmazottakra vonatkozó követelmények

Lásd a HSzSz 5.3.7 pontját.

5.3.8. A személyzet számára biztosított dokumentációk

A személyzet számára biztosítandó dokumentációt a HSzSz 9.1 pontja sorolja fel.

6. Műszaki biztonsági óvintézkedések

A Szolgáltató módosítás ellen védett megbízható rendszereket és termékeket használ.

6.1. Kulcspár előállítás és telepítés

6.1.1. Kulcs-pár előállítás

A Szolgáltató gondoskodik valamennyi általa (saját maga, egyes szervezeti egységei /pl. Címtár, regisztráló szervezet/, illetve más aláírók számára) generált Aláírás létrehozó adat biztonságos és szabványos előállításáról.

A Szolgáltató saját kulcspár előállítása:

- A Szolgáltatónál történő kulcselőállítást fizikailag védett környezetben (lásd 5.1), bizalmi munkakört betöltő személyzet (lásd 5.2.1) végzi, legalább kettős ellenőrzés[34] mellett.

  A kulcselőállítás funkció végrehajtására felhatalmazott személyzet körét a Szolgáltató HSzSz-ének még megfelelve, a lehető legkisebbre korlátozza.
- A Szolgáltató a kulcselőállítást egy olyan eszközön belül hajtja végre, amely megfelel a FIPS 140-1 [13] 3-as szintű követelményeinek.
- A Szolgáltató a kulcs előállítását olyan algoritmussal valósítja meg, melyet jogszabály ismer el erre a célra alkalmasnak.[35]

A Szolgáltató által más felek számára előállított kulcspár előállítás:

- A Szolgáltató által saját szervezeti egységei /Címtár, regisztráló szervezet/ számára előállított kulcsokat biztonságos módon, egy olyan algoritmussal állítja elő, melyet jogszabály ismer el erre a célra alkalmasnak[36].

[34] Két személy együttes jelenlétével
[35] A 2/2002 (IV.26) MeHVM irányelv 1. sz. melléklete felsorolja a megfelelőnek elismert kulcselőállítási algoritmusokat.
[36] A 2/2002 (IV.26) MeHVM irányelv 1. sz. melléklete felsorolja a megfelelőnek elismert kulcselőállítási algoritmusokat.

- A Szolgáltató által az aláírók számára előállított kulcsokat biztonságos módon, egy olyan algoritmussal állítja elő, melyet jogszabály ismer el erre a célra alkalmasnak [37].
- Az Aláírás létrehozó eszköz elkészítését (logikai és fizikai megszemélyesítését) a Szolgáltató ellenőrzi.

6.1.2. Az Aláírás létrehozó adat felhasználóhoz történő eljuttatása

A Szolgáltató amikor kulcsokat generál más felek (regisztráló szervezet és aláírók) számára:

- az általa más felek számára előállított kulcsokat az Előfizető vagy az Aláíró által történő személyes átvételig biztonságos módon tárolja,
- az általa más felek számára előállított magánkulcsot az Előfizetőnek vagy az Aláírónak úgy adja át, hogy a magánkulcs titkossága ne sérüljön,
- az átadást követően csak az Aláíró férhet hozzá saját magánkulcsához,
- a Szolgáltató biztonságosan ellenőrzi az Aláírás létrehozó eszköz elkészítését,
- a Szolgáltató a nem megszemélyesített Aláírás létrehozó eszközt is biztonságosan tárolja.
- a Szolgáltató biztonságosan ellenőrzi az Aláírás létrehozó eszköz kiiktatását és újraaktivizálását,
- a Szolgáltató az Aláírás létrehozó eszköz aktivizálási adatait (PIN kód) biztonságosan készíti el és az aláírás létrehozó modultól elkülönítve osztja szét.

Az Előfizető vagy az Aláíró számára a Szolgáltató:

- olyan algoritmus felhasználásával állítja elő az Aláíró kulcsait, melyet jogszabály a tanúsítványtípusban azonosított kulcshasználatra megfelelőnek ismer el,
- olyan kulcshosszúságot és algoritmust alkalmaz, amelyet jogszabály a tanúsítványtípusban azonosított kulcshasználatra megfelelőnek ismer el.

6.1.3. Aláírás ellenőrző adat eljuttatása a tanúsítvány kibocsátóhoz

[37] A 2/2002 (IV.26) MeHVM irányelv 1. sz. melléklete felsorolja a megfelelőnek elismert kulcselőállítási algoritmusokat.

A Szolgáltató biztosítja a nyilvános kulcs sértetlenségét a kulcspár előállításának helyszínéről (a regisztráló szervezettől) a Tanúsítvány kibocsátásának helyszínére (a hitelesítő szervezethez) történő továbbítás során.

6.1.4. Hitelesítő Szervezet Aláírás ellenőrző adatának eljuttatása a felhasználókhoz

A Szolgáltató saját aláírás ellenőrző (szolgáltatói) adatait elérhetővé teszi az érintett felek részére olyan módon, amellyel biztosítja a Szolgáltató nyilvános kulcsának, valamint az összes ezzel kapcsolatos paraméter sértetlenségét és hitelességét.

6.1.5. Kulcs méretek

A Szolgáltató aláíró saját kulcsára olyan kulcshosszúságot és algoritmust választott, melyet jogszabály ismer el erre a célra alkalmasnak[38].

A Szolgáltató által más felek (regisztráló szervezet, illetve az aláírók) számára generált kulcsok olyan hosszúságúak és olyan algoritmushoz tartozók, melyet jogszabály ismer el erre a célra alkalmasnak[39].

6.1.6. Előfizetői Aláírás ellenőrző adat előállításához használt paraméterek előállítása

A Szolgáltató a nyilvános kulcs paramétereinek előállítása során /beleértve az ehhez szükséges véletlenszám generálást is/ olyan szabványos megoldást használ, melyet jogszabály ismer el erre a célra alkalmasnak[40].

6.1.7. Előfizetői Aláírás ellenőrző adat előállításához használt paraméterek minőségellenőrzése

A Szolgáltató ellenőrzi valamennyi kulcspár előállítása során a paraméterek minőségét a HSzSz-ben meghatározott módon.

---

[38] A 2/2002 (IV.26) MeHVM irányelv 1. sz. melléklete, mely felsorolja az aláíró kulcsokra vonatkozó, megfelelőnek elismert kulcshosszúságokat és algoritmusokat.
[39] Lásd 2/2002 (IV.26) MeHVM irányelv, 1. sz. melléklete.

6.1.8. Szoftveres / hardveres kulcsgenerálás

A Szolgáltató valamennyi kulcspár előállítását egy olyan hardver eszközön belül valósítja meg, amely megfelel a FIPS 140-1 Level 3 szintű követelményeinek.

6.1.9. Kulcs felhasználási célok

A Szolgáltató saját kulcsai használati célja az alábbiak lehetnek:

- tanúsítvány aláírás,
- visszavonási lista aláírás,
- titkosítás.

A Szolgáltató által az aláírók számára előállított kulcsok használati célja elektronikus aláírás lehet[41].

6.2. Aláírás létrehozó adat védelme

A Szolgáltató gondoskodik valamennyi általa (saját maga, regisztráló szervezet, az aláírók számára) előállított magánkulcs titkosságáról és sértetlenségéről.

A Szolgáltató külön aláíró magánkulcsot használ Tanúsítvány aláírásra, és Tanúsítvány visszavonási lista aláírásra, egyúttal ezen kulcsokat semmilyen más célra nem használja.

A Szolgáltató a tanúsítványokat, illetve a Tanúsítvány visszavonási listákat aláíró magánkulcsait fizikailag biztonságos helyszínen használja.

6.2.1. Kriptográfiai modulra vonatkozó szabványok

Hitelesítő szervezet

A hitelesítő szervezet tanúsítványokat és tanúsítvány visszavonási listákat aláíró magánkulcsait egy olyan kriptográfiai hardver modulban állítja elő, tárolja, illetve használja, amely nem kompromittálja a magánkulcs biztonságát, s amely megfelel a FIPS 140-1 [13] 3-as szintű követelményeinek.

[40] Lásd 2/2002 (IV.26) MeHVM irányelve, 1. sz. melléklete.

[41] Ez a tanúsítványtípus elektronikus aláírásra használható kulcsokkal, tanúsítványokkal foglalkozik. A titkosításra használható kulcsokkal a Szolgáltató egy másik tanúsítványtípusa foglalkozik.

Regisztráló szervezet

A regisztráló szervezet magán aláíró kulcsát egy olyan biztonságos kriptográfiai eszközben állítja elő, tárolja, illetve használja, amely nem kompromittálja a magánkulcs biztonságát, s amely megfelel a FIPS 140-1 [13] 2-es szintű követelményeinek.

6.2.2. A több-szereplős ("n-ből m") magánkulcs visszaállítás ellenőrzése

Hitelesítő szervezet

A hitelesítő szervezet magán aláíró kulcsait csak bizalmi munkakört betöltő személyzet állíthatja vissza, legalább kettős ellenőrzés mellett, fizikailag biztonságos környezetben (lásd 5.2.2).

Regisztráló szervezet

A regisztráló szervezet magán aláíró kulcsa nem kerül mentésre, így visszaállítása nem lehetséges[42].

Végfelhasználók

Az előfizetők magán aláíró kulcsa nem kerül mentésre, így visszaállítása nem lehetséges.

6.2.3. Aláírás létrehozó adat letét

A Szolgáltató az Aláíró magán aláíró kulcsait nem tárolja, és nem tartja olyan módon sem, mely lehetővé tenné a (kulcs)adatok későbbi dekódolását[43].

6.2.4. Aláírás létrehozó adat mentése

Hitelesítő szervezet

A hitelesítő szervezet magán aláíró kulcsát csak bizalmi munkakört betöltő személyzet másolhatja le, illetve tárolhatja le, legalább kettős ellenőrzés mellett, fizikailag biztonságos környezetben (lásd az 5.2.2 pontot).

[42] Véletlen megsemmisülése esetén új kulcs előállítás válik szükségessé, ami nem jár a korábban kibocsátott előfizetői tanúsítványok visszavonási kényszerével (mivel a regisztráló szervezet csak a Szolgáltatón belüli kommunikációban ír alá ezen kulcsokkal) .

A hitelesítő szervezet magán aláíró kulcsainak mentett másolataira ugyanolyan szintű biztonsági előírások vonatkoznak, mint a használatban levő kulcsokra.

Regisztráló szervezet

A regisztráló szervezet magán aláíró kulcsának mentése nem lehetséges.

Végfelhasználók

A Szolgáltató által az előfizetőknek előállított magánkulcsok mentése nem lehetséges.

6.2.5. Aláírás létrehozó adat archiválása

Szolgáltató az Aláírás létrehozó adatot nem archivál.

6.2.6. Aláírás létrehozó adat kriptográfiai modulba helyezése

Hitelesítő szervezet

A hitelesítő szervezet magánkulcsait az ezeket felhasználó kriptográfiai hardver modul állítja elő, így ezeket nem kell külön a modulba juttatni.

Arra az időre, amíg a fenti kulcsok a kriptográfiai hardver modult elhagyják átmenetileg, mentési célból, a mentés célját szolgáló tartalék kriptográfiai hardver modulra való áttöltés során, (lásd 6.2.4) a hitelesítő szervezet kódolja magánkulcsait, olyan algoritmust és kulcs hosszat alkalmazva, amely a tudomány mai állása szerint képes ellenállni a kriptográfiai támadásoknak a kódolt kulcs vagy kulcsrészlet teljes hátralévő életciklusában.

A hitelesítő szervezet kriptográfiai hardver modulja kikapcsolt állapotban a magánkulcsokat kódolva tárolja, olyan algoritmust és kulcs hosszat alkalmazva, amely a tudomány mai állása szerint képes ellenállni a kriptográfiai támadásoknak a kódolt kulcs teljes hátralévő életciklusában.

Regisztráló szervezet

A regisztráló szervezet magánkulcsait az ezeket felhasználó kriptográfiai hardver modul állítja elő, így ezeket nem kell külön a modulba juttatni.

[43] Ez a folyamat közismerten a kulcs letétbe helyezése (key escrow) néven ismert, s eleve csak az előfizetői kulcsokra van értelme. (Saját magánkulcsait a Szolgáltató nem „letétbe helyezi", hanem menti, vagy archiválja.)

A regisztráló szervezet magán aláíró kulcsa teljes életciklusában a kriptográfiai eszközben marad, azt semmilyen célból nem hagyja el.

A regisztráló szervezet kriptográfiai hardver modulja kikapcsolt állapotban a magánkulcsokat kódolva tárolja, olyan algoritmust és kulcs hosszat alkalmazva, amely a tudomány mai állása szerint képes ellenállni a kriptográfiai támadásoknak a kódolt kulcs teljes hátralévő életciklusában.

6.2.7. Aláírás létrehozó adat aktiválása

Hitelesítő szervezet

A hitelesítő szervezet (tanúsítványokat és tanúsítvány visszavonási listákat aláíró) magánkulcsai aktivizálását az erre felhatalmazott felhasználó birtokláson és tudáson alapuló kombinált hitelesítési eljárással aktivizálhatja[44].

A hitelesítő szervezet egyéb (a Szolgáltató belső kommunikációjának bizalmasságát és hitelességét védő) magánkulcsai aktivizálását az erre felhatalmazott felhasználó tudáson alapuló hitelesítési eljárással aktivizálhatja.

Regisztráló szervezet

A regisztráló szervezet (az archiválandó regisztrációs adatokat és tranzakciókat aláíró) magánkulcsa aktivizálását az erre felhatalmazott felhasználó tudáson alapuló hitelesítési eljárással aktivizálhatja.

A regisztráló szervezet egyéb (a Szolgáltató belső kommunikációjának bizalmasságát és hitelességét védő) magánkulcsai aktivizálását az erre felhatalmazott felhasználó tudáson alapuló hitelesítési eljárással aktivizálhatja.

Végfelhasználók

Az Aláíró magánkulcsának aktivizálása kívül esik a Szolgáltató felelősségi körén. A magánkulcsot tároló eszközön kódoltan tárolt magánkulcs dekódolásához az Aláírónak tudáson alapuló hitelesítési eljárást kell végrehajtania[45].

6.2.8. Aláírás létrehozó adat deaktiválása

[44] Egy speciális eszköz behelyezésével, valamint felhasználó azonosítója és jelszava megadásával.
[45] A dekódolást végrehajtó funkció jelszavának megadásával.

A hitelesítő és regisztráló szervezetek magánkulcsai aktív állapotának megszüntetése (deaktivizálása) akkor lehetséges, ha a magánkulcsot tároló kriptográfiai hardver modulok szabályos vagy szabálytalan módon kikerülnek az aktivizálást és felhasználást lehetővé tevő állapotból. (Az erre vonatkozó részleteket a HSzSz tartalmazza.)

6.2.9. Aláírás létrehozó adat megsemmisítése

A hitelesítő és a regisztráló szervezet magánkulcsainak megsemmisítése

A Szolgáltató gondoskodik arról, hogy magán aláíró kulcsai ne legyenek felhasználhatók életciklusuk vége után. Különösképpen:

- A Szolgáltató magán aláíró kulcsainak használatát korlátozza oly módon, hogy az összhangban legyen a Tanúsítvány előállításához használt lenyomatoló függvényre, aláíró algoritmusra és kulcshosszra vonatkozó (a 6.1.5 pontban kifejtett) gyakorlatnak[46].
- A Szolgáltató kriptográfiai hardver moduljában tárolt szolgáltatói magán aláíró kulcsokat a hardver modul visszavonásakor megsemmisíti oly módon, hogy a magánkulcsok ne legyenek helyreállíthatók.
- A Szolgáltató magán aláíró kulcsainak megsemmisítésekor azok összes másolatát is megsemmisíti oly módon, hogy a magánkulcsok ne legyenek helyreállíthatók.

A Szolgáltató által az aláírók számára generált magánkulcsok megsemmisítése

- A Szolgáltató – közvetlenül az Aláíró magánkulcsának előállítása után – az aláíró eszközre történő letöltés után magánkulcsot (s annak minden esetleges másolatát) megsemmisíti.
- A Szolgáltató által végrehajtott kulcscsere során – az Aláíró új magánkulcsának Aláírás létrehozó eszközre töltése utáni megsemmisítésén túlmenően – a Szolgáltató gondoskodik arról is, hogy a régi magánkulcs is megsemmisüljön.
- Az Aláró magánkulcsának életciklus végén történő megsemmisítése kívül esik a Szolgáltató felelősségi körén.

[46] Vagyis a jogszabályban meghatározott érvényességi idő lejárta előtt megsemmisíti a magánkulcsokat, figyelembe véve a későbbi jogszabályokban esetlegesen megjelenő érvényesség meghosszabbítást is.

6.3. Kulcs-pár kezelés egyéb aspektusai

6.3.1. Aláírás ellenőrző adat archiválása

A Szolgáltató - Tanúsítvány archiválási szolgáltatása keretén belül – archiválja az előfizetők nyilvános kulcsait.

Az adathordozók egyik példányát Szolgáltató a hitelesítő szervezetben, a másik példányt a földrajzilag távol eső Biztonsági Adattárában tárolja a megőrzési idő végéig.

6.3.2. Aláírás létrehozó és ellenőrző adatok felhasználási ideje

Hitelesítő és regisztráló szervezetek

A Szolgáltató saját magánkulcsai használati periódusa nem haladja meg azok érvényességi idejét, ahogyan azt a 6.2.9 pont is állítja (a Szolgáltató gondoskodik arról, hogy magán aláíró kulcsai ne legyenek felhasználva életciklusuk vége után), összhangban a 6.2.5 pont állításával (a Szolgáltató magán aláíró kulcsot nem archivál).

Végfelhasználók

Az Aláíró magánkulcsának használati periódusa nem haladhatja meg a Tanúsítvány érvényességi idejét, ennek betartása viszont kívül esik a Szolgáltató felelősségi körén. Ennek betartása az Előfizető (s ezen keresztül az Aláíró) kötelessége, ellenőrzése pedig az érintett felek kötelessége.

6.4. Aktiválási adatok

6.4.1. Aktiválási adatok generálása és installációja

A Szolgáltató biztonságosan állítja elő az általa kibocsátott Aláírás létrehozó eszközök aktivizáló adatait.

6.4.2. Aktiválási adatok védelme

A Szolgáltató az általa kibocsátott Aláírás létrehozó eszközök aktivizáló adatait az Aláírás létrehozó eszköztől elkülönítve osztja szét.

6.4.3. Aktiválási adatok egyéb aspektusai

A Szolgáltató az általa kibocsátott Aláírás létrehozó eszközök kiiktatását és újraaktivizálását biztonságosan ellenőrzi.

6.5. Számítógép biztonsági szabályok

6.5.1. Számítógép biztonság technikai követelményei

A Számítógép biztonság technikai követelményeit a MeH 12. ajánlás szerinti fokozott biztonsági osztálybasorolás határozza, amely teljes összhangban van az ITSEC és a Common Criteria ajánlások biztonsági osztályozási rendszerével.

A Szolgáltató gondoskodik arról, hogy az informatikai rendszeréhez való hozzáférés kellően felhatalmazott egyénekre legyen korlátozva. Különösképpen:

- A Szolgáltató védi rendszerei és információi sértetlenségét vírusok, káros és engedély nélküli szoftverek ellen.
- A Szolgáltató biztonságosan kezeli adathordozó eszközeit a sérülés, ellopás és jogosulatlan hozzáférés elleni védelem érdekében.
- A Szolgáltató gondoskodik a felhasználói[47] hozzáférés hatékony nyilvántartásáról a rendszerbiztonság fenntartása érdekében, beleértve a felhasználói hozzáférések naplózását, illetve a hozzáférési jogosultságok kellő időben történő módosítását, áthelyezését.
- A Szolgáltató gondoskodik arról, hogy az információhoz és az alkalmazói rendszer funkciókhoz történő hozzáférés, a hozzáférés ellenőrzési szabályzatnak megfelelően korlátozott legyen, és hogy a Szolgáltató rendszere megfelelő számítógépbiztonsági ellenőrzéseket nyújtson a Szolgáltató szabályzatában azonosított bizalmi munkakörök elkülönítése érdekében, beleértve a biztonsági adminisztrátori és üzemeltetési funkció elkülönítését. Különösképpen a rendszer szolgáltatási programok használatát korlátozza és ellenőrzi szigorúan.
- A Szolgáltató gondoskodik arról, hogy személyzetét sikeresen azonosítsák és hitelesítsék, mielőtt a Tanúsítvány gondozásával kapcsolatos kritikus alkalmazásokat használhatnák.

[47] A felhasználó fogalma itt felöleli a rendszer operátorokat, rendszer adminisztrátorokat és bármely olyan felhasználót, akinek közvetlen hozzáférése van a rendszerhez.

- A Szolgáltató eljárásokat dolgoztat ki és hajtat végre valamennyi olyan bizalmi és adminisztratív munkakörre, amely hatást gyakorol a hitelesítési szolgáltatások nyújtására.
- A Szolgáltató műszaki óvintézkedéseket juttat érvényre (például tűzfalak[48] segítségével), hogy a Szolgáltató belső hálózati tartományai védettek legyenek a harmadik felek számára elérhető külső hálózati tartományoktól.
- A Szolgáltató időben és összehangoltan fellép annak érdekében, hogy gyorsan válaszolni tudjon a váratlan eseményekre, és korlátozza a biztonság megsértésének hatásait. Valamennyi eseményt jelenteni kell az esemény bekövetkezte után, amint az lehetséges.
- A Szolgáltató folyamatos felügyelő és riasztó eszközöket biztosít, hogy képes legyen felismerni és regisztrálni az erőforrásaihoz való jogosulatlan és/vagy szabálytalan hozzáférési kísérleteket, valamint képes legyen ezekre időben reagálni[49].
- A Szolgáltató gondoskodik arról, hogy a tanúsítvány kibocsátást (a Tanúsítvány elérhetővé tételét, nyilvánosságra hozatalát) megvalósító alkalmazás hozzáférés ellenőrzést érvényesítsen a tanúsítványok hozzáadására és törlésére, illetve a kiegészítő információ módosítására vonatkozóan.
- A Szolgáltató gondoskodik arról, hogy a tanúsítvány visszavonás kezelést megvalósító alkalmazás hozzáférés ellenőrzést érvényesítsen a visszavonás állapot információ (hálózatról történő) módosítására vonatkozóan.
- A Szolgáltató gondoskodik arról, hogy az érzékeny adatokat[50] megvédjék az újra felhasználható, jogosulatlan felhasználók által is elérhető tároló egységeken (például törölt adatállományokon) keresztüli felfedés ellen.
- A Szolgáltató biztosítja a személyzet tevékenységéért való felelősségre vonhatóságát.[51]

6.5.2. Számítógép biztonsági értékelések

[48] Ajánlott, hogy a tűzfalakat úgy konfigurálják, hogy azok a Szolgáltató működéséhez nem szükséges protokollokat és hozzáféréseket kiiktassák.
[49] A Szolgáltató erre használhat például egy behatolás észlelő rendszert, vagy hozzáférés ellenőrzést felügyelő és riasztási eszközöket.
[50] Az érzékeny adatok közé tartoznak a regisztrációs információk is.
[51] Például az eseménynapló megőrzésén keresztül.

A Szolgáltató szolgáltatásaira vonatkozóan végrehajtott kockázat elemzés azonosította azokat a kritikus szolgáltatásokat, amelyekhez megbízható informatikai rendszerek kellenek, egyben meghatározta a szükséges értékelési garanciaszinteket.

A Szolgáltató olyan megbízható informatikai rendszereket alkalmaz, melyek a MeH 12. ajánlás szerinti fokozott biztonsági osztálybasorolás követelményeit kielégíti. Ez összhangban van az ITSEC F-B1/E3, illetve a Common Criteria ajánlás AL*4* biztonsági osztályok követelményeivel.

6.6. Életciklus technikai szabályok

6.6.1. Rendszerfejlesztési szabályok

A Szolgáltató gondoskodik arról, hogy az általa, illetve a nevében végzett valamennyi rendszerfejlesztési projektjében a biztonság követelményeit már a tervezési és követelmény-meghatározási fázisban figyelembe vegyék, annak érdekében, hogy a biztonság beépüljön az informatikai rendszerekbe.

A Szolgáltató konfiguráció kezelési eljárásokat alkalmaz valamennyi működő szoftvere esetében a kibocsátásokra, a módosításokra és a sürgős szoftver javításokra vonatkozóan.

Az IT életciklusra vonatkozó rendszerfejlesztési szabályokat a Szolgáltató társasági szintű Informatikai biztonságpolitikája és az Informatikai Biztonsági Szabályzat tartalmazza, amelyek pontosan meghatározzák az előkészítés, a projekt, az üzemeltetés és a visszavonás/rekonstrukció ciklus időszakok feladatait és az alkalmazott módszertanokat.

6.6.2. Biztonságkezelési szabályok

A Szolgáltató olyan eszközöket és eljárásokat alkalmaz, melyek garantálják a kritikus szolgáltatásait (lásd 6.5.2 pont) megvalósító megbízható informatikai rendszereire az operációs rendszer beállítások, valamint a hálózati konfiguráció biztonságát, egyúttal az alkalmazott biztonsági mechanizmusok sértetlenségének, helyes működésének ellenőrzését.

A biztonságkezelési szabályok a Szolgáltató társasági szintű Informatikai biztonságpolitikája, valamint a társasági és a rendszer szintű Informatikai Biztonsági

Szabályzatok tartalmazzák. A Szolgáltató hitelesítés támogató informatikai rendszere vonatkozásában a rendszer szintű szabályzat a Biztonsági Szabályzat.

6.6.3. Életciklus biztonsági értékelések

A Szolgáltató által alkalmazott megbízható informatikai rendszerek a MeH 12. ajánlás fokozott biztonsági osztálya követelményeinek megfelel, amely azonos szintű az ITSEC F-B1/E3, illetve a Common Criteria EAL4 szintnek.

6.7. Hálózati biztonsági szabályok

A Szolgáltató gondoskodik arról, hogy informatikai rendszerében megfelelő hálózatbiztonsági ellenőrzésekre kerüljön sor. Az érzékeny adatokat megvédi, amikor azok átvitele nem biztonságos hálózatokon keresztül történik.

A regisztrálással kapcsolatosan:

- A regisztrációs adatok bizalmasságát és sértetlenségét megvédik, különösen az Előfizetővel/Aláíróval folytatott külső, illetve a Szolgáltató egyes komponensei közötti belső adatcsere során.
- A Szolgáltató (a hitelesítő szervezeten keresztül) ellenőrzéssel biztosítja, hogy regisztrációs adatokat csak általa elismert, azonosságában hitelesített regisztrációs szolgáltatókkal cserél.

A tanúsítvány előállítással és visszavonás kezeléssel kapcsolatosan:

- A Szolgáltató gondoskodik arról, hogy a helyi hálózati komponensek fizikailag biztonságos környezetben legyenek és konfigurációikat időszakonként auditálják.
- A Szolgáltató folyamatos felügyelő és riasztó eszközöket biztosít, hogy képes legyen felismerni, regisztrálni az erőforrásaihoz a hálózatról történő hozzáférésre irányuló jogosulatlan és/vagy szabálytalan próbálkozásokat, illetve képes legyen időben reagálni ezekre.

A Tanúsítvány kibocsátásával kapcsolatosan:

- A Szolgáltató gondoskodik arról, hogy a tanúsítvány kibocsátást (a Tanúsítvány elérhetővé tételét, nyilvánosságra hozatalát) megvalósító alkalmazás hozzáférés ellenőrzést érvényesítsen a tanúsítványok hozzáadására és törlésére, illetve a kiegészítő információ módosítására vonatkozóan.

A tanúsítvány visszavonás kezeléssel kapcsolatosan:

- A Szolgáltató gondoskodik arról, hogy a tanúsítvány visszavonás kezelést megvalósító alkalmazás hozzáférés ellenőrzést érvényesítsen a visszavonás állapot információ hálózatról történő módosítására vonatkozóan.

6.8. Kriptográfiai modul ellenőrzése

A Szolgáltató gondoskodik a kriptográfiai hardver biztonságáról annak teljes élettartama alatt. Különösképpen gondoskodik arról, hogy:

- a Tanúsítványt és a visszavonási állapotot aláíró kriptográfiai hardvert nem manipulálják szállítás közben,
- a Tanúsítványt és a visszavonási állapotot aláíró kriptográfiai hardvert nem manipulálják tárolás közben,
- a Szolgáltató aláíró kulcsainak kriptográfiai hardverben történő installálása, aktivizálása, mentése és visszaállítása legalább két bizalmi munkakört betöltő alkalmazott együttes jelenlétét kívánja meg,
- a Tanúsítványt és a visszavonási állapotot aláíró kriptográfiai hardver helyesen működik,
- a Szolgáltató kriptográfiai hardverén tárolt szolgáltatói magán aláíró kulcsokat az eszköz visszavonásakor megsemmisítik.

7. Tanúsítvány és kulcs-visszavonási profil

7.1. Tanúsítvány profil

A Szolgáltató által kibocsátott tanúsítványok megfelelnek:

1. az RFC 2527 szabványban leírt X.509 3-as verziójú tanúsítványoknak,
2. az RFC 3039 szabványban leírt minősített tanúsítványoknak,
3. az ETSI TS 101 862 szabványban leírt minősített tanúsítványoknak.

7.1.1. Alap mezők

Megfelelnek a 7.1 fejezet 1.-3. feltételeknek. Az alap mezők értékei a HSzSz 7.1 pontja szerint.

7.1.2. Tanúsítvány kiterjesztések

Megfelelnek a 7.1 fejezet 1.-3. feltételeknek. A Szolgáltató az ITU-T X.509 ajánlás 3. verziójának megfelelő Tanúsítvány kiterjesztéseket támogatja. A kiterjesztések a HSzSz 7.1.2 pontja szerint.

A Szolgáltató a Tanúsítványban álnév feltüntetését vállalja.

A szabályzat kiterjesztés feldolgozásáért az Előfizető és Érintett fél alkalmazása és eljárása felelős. A Szolgáltató semmilyen körülmények között nem hibáztatható a kiterjesztés, vagy a szabályzatokban foglaltak figyelmen kívül hagyása, téves értelmezése miatt.

7.2. Kulcs-visszavonási profil

A Szolgáltató által kibocsátott tanúsítvány visszavonási listák megfelelnek:

1. az ITU X.509 *"Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer"* ajánlásának.

RFC 2527 szabványban leírt X.509 2-as verziójú tanúsítvány visszavonási listáknak.**Alap mezők**

Megfelelnek a 7.2 fejezet 1.-2. feltételeknek. Az alap mezők értékei a HSzSz 7.2 pontja szerint.

7.2.2. Verzió szám(ok)

Megfelelnek a 7.2 fejezet 1.-2. feltételeknek. A Szolgáltató ITU-T X.509 ajánlás 2. verziója szerinti tanúsítvány visszavonási listákat bocsát ki.

7.2.3. „Tanúsítvány visszavonási lista" és „Tanúsítvány visszavonási lista bejegyzési" kiterjesztések

Megfelelnek a 7.2 fejezet 1.-2. feltételeknek. A kiterjesztések értékei a HSzSz 7.2 pontja szerint.

A visszavonási lista kiterjesztés és visszavonás bejegyzési kiterjesztések feldolgozásáért az Előfizető és Érintett fél alkalmazása és eljárása felelős. Szolgáltató semmilyen körülmények között nem hibáztatható a kiterjesztések figyelmen kívül hagyása vagy téves értelmezése miatt.

8. HP/HSzSz adminisztráció

A Szolgáltató rendelkezik egy olyan HSzSz-el, amely a minősített tanúsítványokra, és valamennyi, a HSzSz-ben közölt állítást megvalósító gyakorlatra és eljárásra vonatkozik.

A HSzSz meghatározza a Szolgáltató szolgáltatásait támogató valamennyi külső szervezetre vonatkozó kötelezettségeket, beleértve az alkalmazandó szabályzatokat is.

8.1. A HP/HSzSz változatkezelési eljárások

A Szolgáltató egy felülvizsgálati folyamatot határoz meg, mely kiterjed a Hitelesítési Politika (HP) és a HSzSz gondozására is.

A Szolgáltató időben értesítést tesz közzé az általa támogatott HP-ben, illetve HSzSz-ben tervezett változtatásokról, majd a 8.3 pont szerint történő jóváhagyást követően az átdolgozott HP/HSzSz-t a 8.2 pontban előírtak szerint haladéktalanul hozzáférhetővé teszi.

8.2. Közzétételi és tájékoztatási elvek

A Szolgáltató az általa támogatott HP-t, valamint HSzSz-t és egyéb más fontos dokumentációját az előfizetők és az érintett felek rendelkezésére bocsátja, a tanúsítványtípusnak való megfelelés felméréséhez szükséges mértékig[52].

A Szolgáltató a Tanúsítvány használatával kapcsolatos kikötéseit és feltételeit az összes Előfizető és potenciális érintett fél számára megismerhetővé teszi, a 2.6.1 pontban meghatározottak szerint.

8.3. HP/HSzSz elfogadási eljárások

A HP-re vonatkozóan:

- Formailag megfelel az RFC 2527 szabványnak.
- A tanúsítványtípus tartalmilag megfelel az európai ETSI TS 101 456 szabvány **MTT** tanúsítványtípusokkal szemben támasztott minimális követelményeinek.

[52] Általában a Szolgáltatóval szemben nem követelmény, hogy szabályzatait teljes részletességgel nyilvánosságra hozza.

- A Szolgáltató jóváhagyás előtt megvizsgálja a HP előző pontokban meghatározott követelményeknek való megfelelőségét.
- A HP jóváhagyására[53] a Szolgáltató felsőszintű irányító testülete rendelkezik végső hatáskörrel és felelősséggel.

A HSzSz-re vonatkozóan:

- A HSzSz és formailag megfelel a HP-nek[54].
- A Szolgáltató jóváhagyás előtt megvizsgálja a HSzSz-t a HP-nek való megfelelőség szempontjából.
- A HSzSz jóváhagyására a Szolgáltató felsőszintű irányító testülete rendelkezik végső hatáskörrel és felelősséggel.
- A Hírközlési Felügyelet nyilvántartásba veszi a Szolgáltató által jóváhagyott és bejelentett HSzSz -t.

[53] vagy esetlegesen a Hírközlési Felügyelet által már nyilvántartásba vett tanúsítványtípusok közül történő kiválasztására

[54] A tartalmi és formai megfelelés azt jelenti, hogy a HSz „mit valósít meg a Szolgáltató" típusú állításait a HSzSz „hogyan valósítja meg ezeket" típusú leírásai ellentmondás mentesen és hasonló szerkezeti felépítéssel részletezik.

9. Hivatkozások és meghatározások

9.1. Hivatkozások

Hivatkozott törvények, kormányrendeletek, MeH rendeletek:

- 2001. évi XXXV. törvény az elektronikus aláírásról,
- 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről,
- 151/2001. (IX. 1.) Korm. rendelet a Hírközlési Felügyeletnek az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól,
- 15/2001. (VIII. 27.) MeHVM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról.
- 2/2002. (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről.
- 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról,
- 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról,
- 1995. évi CXXII. törvény a polgárok személyes adatainak nyilvántartásáról szóló 1992. évi LXVI. törvény módosításáról szóló törvény.

A Szolgáltató hivatkozott Szabályzatai:

- A MÁV INFORMATIKA Kft. Szervezeti és Működési Szabályzata,
- A MÁV INFORMATIKA Kft. Iratkezelési Szabályzata
- A MÁV INFORMATIKA Kft. Titokvédelmi Szabályzata
- A MÁV INFORMATIKA Kft. informatikai Biztonságpolitikája
- A MÁV INFORMATIKA Kft. Informatikai Biztonsági Szabályzata
- PKI Üzleti Egység Biztonsági Szabályzata
- Tanúsítvány politikák
- Általános Szerződési Feltételek
- Előfizetői Szerződés Minta

- Üzletmenet-folytonossági Terv
- Üzemeltetési Utasítás

Hivatkozott ajánlások, szabványok:

- ITU-T X.509 "Information technology - Open Systems Interconnection - The Directory: Public -key and attribute certificate frameworks" ajánlás 3. verziója,
- Internet Közösség RFC 2459 ajánlása,
- Internet Közösség RFC 2527 ajánlása,
- Internet Közösség RFC 3039 ajánlása,
- Európai Unió ETSI TS 101 456 szabvány,
- Európai Unió ETSI TS 101 862 szabvány,
- NIST FIPS 140-1 Level 1-3,
- American Bar Association (ABA) PKI Assessment Guidelines (PAG),
- a CWA 14167-1, és a CWA 14172-1,-2,-3,-4 CEN Workshop Agreement-ek
- MeH 12. ajánlás,
- ITSEC,
- Common Criteria.

9.2. Meghatározások

Aláírás ellenőrző: az Aláíró által elektronikus aláírással ellátott elektronikus irat címzettje.

Aláírás ellenőrző adat: Olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), melyet az elektronikus iratot vagy dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ.

Aláírás létrehozó adat: Olyan egyedi adat (jellemzően kriptográfiai magánkulcs), melyet az Aláíró az elektronikus aláírás létrehozásához használ.

Aláírás létrehozó eszköz: Szoftver vagy hardver, melynek segítségével az Aláíró az Aláírás létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.

Aláírás létrehozó rendszer: Az a rendszer, illetve alkalmazás az aláírás létrehozási környezeten belül, amelyik egy Aláírás létrehozó eszközt használ fel elektronikus aláírás létrehozásához.

Aláíró: egy Tanúsítványban azonosított entitás, aki a Tanúsítványban szereplő nyilvános kulcsnak megfelelő magánkulcsot birtokolja.

Aláíró környezet: Az a fizikai és logikai környezet, melyben az aláírási folyamat lezajlik, és amely egy Aláírás létrehozó rendszert tartalmaz egy Aláírás létrehozó eszközzel, az Aláíróval és az Aláíró által kezelt rendszerelemekkel.

Aláíró eszköz: Megegyezik az Aláírás létrehozó eszközzel.

Biztonságos környezet: Olyan fizikai környezet, mely védett illetéktelen hozzáféréstől, és bizonyos mértékig tűz, víz és egyéb katasztrófaeseményektől, egyéb erőszakos behatásoktól.

Címtár: X. 500 alapú címtár, amelyben a tanúsítványok, az állapotuk, a visszavonási listák (CRL) a HP 2.6.2 pontjában megadott ciklusidővel frissülnek. Tartalma nyilvánosan elérhető LDAP-al vagy web lapról.

Címtár szolgáltatások: A hitelesítő szervezet a regisztráló szervezeteken keresztül fogadja és feldolgozza a tanúsítványokkal kapcsolatos változások adatait, nyilvántartást vezet a tanúsítványok aktuális helyzetéről, esetleges felfüggesztéséről, illetve visszavonásáról. Ezeket, valamint az Aláírás-ellenőrző adatokat, továbbá a visszavont tanúsítványok nyilvántartását (CRL) Internet segítségével bárki számára hozzáférhető és folyamatosan elérhető módon közzéteszi a Címtárban.

Elektronikus aláírás: elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt és azzal elválaszthatatlanul összekapcsolt elektronikus adat, illetőleg dokumentum.

Ellenőrzési lépések: Az elektronikus aláírás ellenőrzésekor kötelezően elvégzendő műveletsor.

Előfizető: Az a személy vagy szervezet, amely Szolgáltatóval érvényes Előfizetői Szerződéssel rendelkezik hitelesítés-szolgáltatás igénybe vételére, és így a Szolgáltató által kiadott Tanúsítvány tulajdonosának tekinthető.

Érintett fél: Az elektronikus dokumentum fogadója, aki egy adott Tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el.

Fokozott biztonságú elektronikus aláírás: Elektronikus aláírás, amely megfelel a következő követelményeknek:

- alkalmas az Aláíró azonosítására és egyedülállóan hozzá köthető,
- olyan eszközzel hozták létre, amely kizárólag az Aláíró befolyása alatt áll,
- a dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően az iraton, illetve dokumentumon tett – módosítás érzékelhető.

Fokozott biztonságú szolgáltató: a Hírközlési Felügyeletnél bejelentett és nyilvántartási számmal rendelkező Hitelesítés Szolgáltató, amely a 2001. évi XXXV. törvényben, a 16/2001 (IX. 1.) MeHVM rendeletben és a 151/2001. (IX. 1.) Korm. rendeletben foglaltaknak megfelel és fokozott biztonságú Aláírás létrehozó adatot és Tanúsítványt bocsát ki.

Hitelesítő szervezet: a hitelesítés szolgáltató azon egysége, mely a hitelesítés-szolgáltatás hitelesítő kulccsal folytatott tevékenységét végzi. A központ fizikailag egy telephelyre koncentráltan, védett, biztonságos körülmények között működik.

Elsődleges (Root) hitelesítő szervezet: az elsőnek létrehozott, fizikailag is működő hitelesítő szervezet, amely az alája rendelt másodlagos hitelesítő központokat hitelesíti,

Produktív hitelesítő szervezet: az Elsődleges hitelesítő szervezet által létrehozott logikailag vagy fizikailag létező hitelesítő szervezet, amely egy adott alkalmazási, szervezeti, földrajzi stb. területre ad ki tanúsítványokat.

Hitelesítés szolgáltató: Személy (szervezet), amely a hitelesítés szolgáltatás keretében azonosítja az igénylő személyét, Tanúsítványt bocsát ki, nyilvántartásokat vezet, fogadja a tanúsítványokkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a tanúsítványokhoz tartozó szabályzatokat, az aláírás ellenőrző adatokat és a Tanúsítvány visszavonási listát.

Igénylő: Az a személy vagy szervezet, amely Szolgáltatóhoz fordul a hitelesítés-szolgáltatás igénybe vétele céljából. Az Igénylő Előfizetői Szerződés megkötése után válik Előfizetővé.

Kompromittálódás: Az az eset, amikor az Aláírást létrehozó eszköz használatára, illetve az aláírás elhelyezésére arra nem jogosított személy képessé válik.

(Kriptográfiai) Kulcs: Kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete az elektronikus aláírás előállításához, illetőleg ellenőrzéséhez szükséges.

Kriptográfiai modul: Hardver alapú biztonsági megoldás, amely alkalmas beépített eljárások segítségével biztonságos kulcsgenerálásra és tárolásra.

Kulcshordozó eszköz: Aláírás létrehozó adat tárolására szolgáló eszköz.

Magánkulcs aktiválása: A magánkulcs aktiválása az a folyamat, melynek során a jogosult – különböző azonosító elemek pl. jelszó, PIN kód megadásával – engedélyezi, hogy a leolvasóba helyezett magánkulcs megkezdje üzemszerű működését. Az aktiválás általában a magánkulcsot igénylő aláíró környezetben (dokumentum aláíró-, levelező rendszer) történik, és érvényes lehet a visszavonásig (deaktiválásig) illetve egyszeri használatra.

Magánkulcs deaktiválása: A magánkulcs deaktiválása az a folyamat, melynek során a magánkulcs üzemszerű működése megszüntetésre kerül. Ez olyan kulcshordozó esetén, amikor a kulcs üzemszerű működés során nem hagyja el a kulcshordozó eszközt, történhet a kulcshordozó olvasóból történő eltávolításával, más esetekben a kulcshordozó eszköz aláíró környezetből való eltávolításával, vagy az alkalmazásból való kilépéssel.

Minősített elektronikus aláírás: olyan - fokozott biztonságú - elektronikus aláírás, amely Biztonságos aláírás létrehozó eszközzel készült, és amelynek hitelesítése céljából minősített Tanúsítványt bocsátottak ki.

Minősített szolgáltató: amelyet a Hírközlési Felügyelettől a minősítési eljárás után a minősített szolgáltatóként bejegyzett, azaz megfelelt az elektronikus aláírásról szóló 2001. évi XXXV. törvény 8. § (4) és (5) bekezdésekben meghatározott személyi, technikai és egyéb feltételeknek és a 6. § (1) bekezdésében meghatározott szolgáltatást kíván nyújtani.

Minősített tanúsítvány: az elektronikus aláírásról szóló 2001. évi XXXV. törvény 2. számú mellékletében foglalt követelményeknek megfelelő olyan Tanúsítvány, melyet minősített szolgáltató bocsátott ki.

Nem minősített tanúsítvány: a CWA 14167-1 CEN Workshop Agreement szerint olyan Tanúsítvány, amely

- Az Európai Közösség (EK) 1999/93. direktívájának 5.2 cikkelyével összhangban levő elektronikus aláírást tanúsítja,
- A Szolgáltató megbízható informatikai rendszerén belül használt.

Az EK 1999/93 direktíva 5.2 cikkelye szerint a Tagállamoknak biztosítania kell, hogy egy elektronikus aláírás jogi eljárásban nem utasítható vissza, mint törvényesen hatályos és elfogadható bizonyíték csupán azon az alapon, mert az

- elektronikus formában létezik, vagy
- nem minősített tanúsítványra alapozott, vagy
- nem egy akkreditált hitelesítés-szolgáltató által kibocsátott minősített tanúsítványra alapozott, vagy
- nem Biztonságos aláíró eszközzel hozták létre.

Nyilvános (publikus) kulcsú infrastruktúra: Az elektronikus aláírás létrehozására, ellenőrzésére, kezelésére szolgáló, aszimmetrikus kulcspárt alkalmazó infrastruktúra, beleértve a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.

Regisztráló szervezetek: A regisztráló szervezetek a Szolgáltató és a vele szerződése alapon együtt működő Társaságok azon szervezeti egységei, amelyek az előfizetők adatainak regisztrációját, ellenőrzését, az igénylő személyazonosságának és hitelességének megállapítását, a tanúsítvány kérelmek összeállítását, a hitelesítő szervezethez történő továbbítását, és egyéb azonosítási, tanúsítványmenedzsment és adminisztrációs feladatokat látnak el a HP-ben és az Általános Szolgáltatási Feltételekben előírtak szerint.

Regisztrációs adatok: Azon információk, adatok összessége, amelyeket a Szolgáltató a tanúsítványkiadás érdekében az Előfizetőről begyűjt.

Szolgáltatás: Elektronikus aláírás hitelesítés-szolgáltatás (röviden: hitelesítés-szolgáltatás) és Aláírás létrehozó adat előállítása és elhelyezése az Aláírás létrehozó adatot tároló eszközön.

Szolgáltatási szabályzat: A hitelesítés-szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó nyilvános dokumentum.

Szolgáltató: A MÁV INFORMATIKA Kft. és a hitelesítési szolgáltatásban tevékenyen részt vevő, vele szerződéses kapcsolatban álló partnerek.

Tanúsítvány: A hitelesítés-szolgáltató által kibocsátott igazolás, amely az Aláírás ellenőrző adatot az elektronikus aláírásról szóló törvény szerint egy meghatározott személyéhez kapcsolja és igazolja e személy személyazonosságát.

Tanúsítvány frissítés: amikor a Szolgáltató érvényes magánkulcsával az új Tanúsítványban a Tanúsítvány tulajdonosának változatlan (régi) nyilvános kulcsát és változatlan egyéb adatait írja alá új érvényességi időtartamra,

Tanúsítvány aktualizálás: amikor a Szolgáltató érvényes magánkulcsával az új Tanúsítványban a Tanúsítvány tulajdonosának változatlan (régi) nyilvános kulcsát és megváltozott új adatait írja alá új érvényességi időtartamra,

Tanúsítvány kulcscsere: amikor a Szolgáltató érvényes magánkulcsával az új Tanúsítványban a Tanúsítvány tulajdonosának új nyilvános kulcsát és változatlan egyéb adatait írja alá új érvényességi időtartamra.

Tanúsítványok osztályai: A tanúsítványok megbízhatósága szerinti megkülönböztetés. A kibocsátást megelőző ellenőrző lépések biztonságosságának jelzésére is szolgál (a jelenleg létező osztályok: minősített, fokozott biztonságú, szolgáltatói, teszt).

Tanúsítványtípus: a hazai joganyagban a nemzetközi ajánlásokban és szabványokban használt Certficate Policy (tanúsítványpolitika) fogalomnak felel meg. Más szóhasználattal *hitelesítési szabályzat*, szabálygyűjtemény, amely egy Tanúsítvány felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy csoportja számára.

A tanúsítványtípus (hitelesítési szabályzat) döntő mértékben a Szolgáltatóra vonatkozó szabályokat (*mit kell betartani*) tartalmazza (de érinti a szolgáltatásokat igénybe vevő felek kötelezettségeit is).

Az ETSI TS 101456 európai szabvány a *tanúsítványtípus* fogalmat a minősített tanúsítványok következő két csoportjára használja:

- MTT (ang: Qualified Certificaton Policy /QCP/): minősített tanúsítványtípus, mely nem követeli meg az Aláírótól Biztonságos aláírás létrehozó eszköz használatát,
- MTT+BALE (ang: QCP + Secure-Signature-Creation Device /SSCD/): minősített tanúsítványtípus, mely megköveteli az Aláírótól Biztonságos aláírás létrehozó eszköz használatát.

Tanúsítvány visszavonási lista: Valamely okból felfüggesztett vagy visszavont, azaz érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, amelyet a hitelesítés-szolgáltató bocsát ki.