MÁV INFORMATIKA

Kereskedelmi, Szolgáltató és Tanácsadó Kft.

Trust&Sign®

Hitelesítés Szolgáltatási Szabályzat a Minősített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz

Verziószám	**2.2**
Hatálybalépés dátuma	**2003. augusztus 15.**

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	Hitelesítés Szolgáltatási Szabályzat a Minősített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz (HSzSz)*
HSzSz verziószám	2.2
Üzemelő PKI szoftver verziószám (Technikai azonosító)	Trust&Sign QCAV1.0
Üzemelő időbélyegzés szoftver verziószám (Technikai azonosító)	Trust&Sign TSAV1.0
HIF regisztrációs szám	
HSzSz objektum azonosító (OID)	1.3.6.1.4.1.14868.1.2
Első hatálybalépés időpontja	2003. január 31.
Aktuális változat hatálybaléptetés időpontja	2003. augusztus 15.
Következő felülvizsgálat időpontja	2004. július 31.

* A MÁV INFORMATIKA Kft. Hitelesítés Szolgáltatási Szabályzata az elektronikus aláírásról szóló 2001. évi XXXV. törvény szerint előírt Szolgáltatási Szabályzat a Hírközlési Felügyelet által meghatározott nyilvános körben kibocsátott Minősített tanúsítványtípusra (**MTT**), a Biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő Minősített tanúsítványtípusra (**MTT+BALE**), és időbélyegzés szolgáltatáshoz, amely a hazai gyakorlatnak megfelelően az Internet Közösség RFC 2527 ajánlásában és az EU ETSI TS 101 456 szabványában javasolt Certificate Practice Statement (CPS) szerkezetet követi

HSzSz verziók

Verzió	Dátum	A változás leírása	Hatálybalépés dátuma	Készítette
1.0	2002.09.30	A fokozott biztonságú szolgáltatói regisztrálásra előkészített, a HIF részére átadott változat.		Bodlaki Ákos
1.0.1	2002.10.03	A PKI Projekt vezető észrevételei szerint módosítva és részére átadott változat.		Bodlaki Ákos
1.0.2	2002.10.03	A HIF részére átadott változat		Bodlaki Ákos Tóth Elemér
1.0.3	2002.10.25	Fokozott biztonságú szolgáltatás induló HSzSz. a HIF és Néder Ferenc észrevételeivel, HIF mintával módosított változat		Bodlaki Ákos
1.0.4	2002.10.29	V1.2 véleményezés alapján módosított változat		Bodlaki Ákos
2.0	2002.11.29	HSzSz minősített tanúsítványtípusokra, véleményezésre átadott változat		Bodlaki Ákos
2.1	2003.03.31.	A minősítési eljárásra átadott változat kiegészítve és módosítva a HIF észrevételeivel	2003.04.06.	Bodlaki Ákos
2.2	2003.07.30	Időbélyegzés szolgáltatás minősítési eljárására beadott 1.0 változattal kapcsolatos észrevételekkel módosítva.	2003.08.15.	Bodlaki Ákos

TARTALOMJEGYZÉK

1. Bevezetés

E dokumentum a MÁV INFORMATIKA Kft. (továbbiakban Szolgáltató) minősített elektronikus hitelesítés szolgáltatására vonatkozó eljárásrendet és az egyéb működési szabályokat tartalmazza.

A Szolgáltató a minősített hitelesítés szolgáltatást a vele előfizetői szerződéses viszonyban álló igénybevevők részére szolgáltatja.

A minősített elektronikus aláírással kapcsolatos szolgáltatások (továbbiakban: szolgáltatás) 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 (továbbiakban: hitelesítés szolgáltatás),
- Aláírás-létrehozó eszközön az Aláírás létrehozó adat elhelyezése,
- időbélyegzés.

A HSzSz további fejezeteiben a „*szolgáltatás*” kifejezés alatt a fenti részszolgáltatások együttese értendő.

A szolgáltatások részletezése a 1.3.6.2 pontban olvasható.

Ezen szolgáltatásokat a Szolgáltató minősített szinten szolgáltatja.

A Hitelesítés Szolgáltatási Szabályzat (továbbiakban: HSzSz) jelen aktuális verziója a PKI alkalmazás mindenkori technikai azonosítójával van összerendelve, azaz a HSzSz-ben foglaltak a technikai azonosítóval azonosított PKI alkalmazásra vonatkoznak.

Az aktuális PKI alkalmazás technikai azonosító: **Trust&Sign QCA V1.0.**

Az aktuális időbélyegzés alkalmazás technikai azonosító: **Trust&Sign TSA V1.0.**

A szolgáltatások védett márkaneve: **Trust&Sign**

1.1. Alapok

1.1.1. Szabályzat célja

Jelen HSzSz célja, hogy összefogja azokat az előírásokat, adatokat és információkat, melyeket a Szolgáltatóval valamilyen módon kapcsolatba kerülő feleknek tudni kell vagy érdemes. Biztosítja a Szolgáltató működésének átláthatóságát, s lehetővé teszi a felhasználók számára, hogy megállapítsák azt, hogy az ismertetett szolgáltatási gyakorlat, valamint a kibocsátott tanúsítványok mennyiben felelnek meg az elvárásaiknak. A HSzSz és egyéb, a HSzSz-ben hivatkozott dokumentumok, ajánlások, szabványok tartalmának megismerése után, a Tanúsítvány, illetve az időbélyeg elfogadóinak egyértelműen meg kell tudni állapítani az elektronikus aláíráshoz, illetve az időbélyeghez kapcsolódó Tanúsítvány ellenőrzésének módját, az általa garantált hitelesség és biztonság mértékét és az erre vonatkozó technikai, üzleti és pénzügy garanciákat, jogi felelősség vállalásokat.

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

1.1.2. Szabályzat tartalma

A HSzSz 1. fejezet (Bevezetés):

- ismerteti a Szolgáltatóval kapcsolatos adminisztratív adatokat,
- eligazítást ad a dokumentum szerepét és a szolgáltatás mibenlétét illetően,
- megnevezi azon szabványokat, ajánlásokat és előírásokat, melyeket a szabályzat formai megjelenésében és tartalmilag követ,
- felsorolja a szabályzat alapján kibocsátható tanúsítvány osztályokat és típusokat,
- ismerteti a szabályzat egyéb dokumentumokhoz való viszonyát, tájékoztatást ad a Szolgáltató által nyújtott szolgáltatásokról, és ezek alkalmazói közösségéről.

A 2. fejezet (Általános rendelkezések) tájékoztat

- a Szolgáltató és annak egységeinek, valamint a minősített szolgáltatásokkal kapcsolatba kerülő szereplőknek a kötelezettségeiről, jogairól, felelősségéről és ennek korlátozásáról,

- felsorolja a Szolgáltató által publikált információkat, dokumentumokat és adatokat a publikálás helyével, gyakoriságával és elérhetőségével, s az esetleges korlátozásokkal, valamint az információk használatára vonatkozó követelményekkel,
- összefoglaló jellegű felvilágosítást ad a Szolgáltató által kezelt adatokról, az adatkezelés céljáról, a közzétett adatokról és azok jogalapjáról, az egyes adatok törlési határidejéről,
- ismerteti a Szolgáltató hitelesítő központjainak saját root hitelesítő központ által történő, saját tanúsításával kapcsolatos információkat.

A 3. fejezet (Azonosítás és hitelesítés)

- a tanúsítványok igényléséhez kapcsolódó előfizetői regisztráció menetét ismerteti, a regisztrációval kapcsolatos tájékoztatással, a regisztrációs adatok összegyűjtésével, és egyéb részletekkel,
- a kezdeti regisztráció kapcsán felsorolja
  - az elnevezés során követett szabványokat és szabályokat,
  - a különböző név formátumok értelmezését,
  - a nevek egyediségének biztosítását,
- ismerteti a név igénylési viták feloldását,
- leírja a Tanúsítvány megújításának kérelmezését, hitelesítését, és elbírálását, valamint a megújítás menetét;
- kifejti a Tanúsítvány visszavonásának kérelmezését, hitelesítését, elbírálását, és végrehajtását.

A 4. fejezet (A működésre vonatkozó követelmények) leírja

- a Szolgáltató által követett gyakorlatot és a támasztott követelményeket a tanúsítványok igénylése, kibocsátása, elfogadása, felfüggesztése, visszavonása és kezelése, valamint az időbélyegzés kapcsán,
- tájékoztat a szolgáltatás megszűnésének körülményeiről, a felek ez esetre vonatkozó jogairól és kötelességeiről, a tanúsítványok kezeléséről, az előfizetők értesítéséről, és az archív adatok kezelésére vonatkozó eljárásokról; valamint ismerteti Szolgáltató naplózási, archiválási és katasztrófa elhárítási eljárásait.

Az 5. fejezet (Fizikai, eljárásrendi, és humán biztonsági szabályozások) leírja azokat a szabályokat, melyek a szolgáltatás környezetének, a bizalmi tevékenységek végzésének és a megfelelő munkatársak rendelkezésre állásának biztonsági előírásait határozzák meg.

A 6. fejezet (Műszaki biztonsági óvintézkedések) ismerteti

- a kulcs-párok generálásának, a magánkulcs címzetthez juttatásának, a 1.3.2 pontban definiált Hitelesítő Szervezet (amely lehet a Szolgáltató maga vagy egy fölé rendelt Hitelesítő Szervezet) nyilvános kulcsának a felhasználókhoz való eljuttatásának szabályait, s a kulcsokkal kapcsolatos technikai követelményeket,
- megadja a Szolgáltató és az előfizetők magánkulcsának, valamint az időbélyeg aláíró kulcs védelmére vonatkozó előírásokat, a magánkulcs kriptográfiai modulba helyezésének módját, aktiválását, deaktiválását és megsemmisítését,
- tájékoztatást ad a kulcs-párok kezelésének egyéb aspektusairól, mint például a nyilvános kulcs archiválására vonatkozó előírásokról, vagy a nyilvános és magánkulcs felhasználási idejéről,
- leírja a magánkulcsok védelmére szolgáló aktiválási adatok generálását, installációját, s védelmét, valamint számítógépes és hálózati biztonsági, életciklus technikai eljárásokat ismertet.

A 7. (Tanúsítvány és kulcs-visszavonási profil) fejezet ismerteti

- a kiadott tanúsítványok alap és opcionális mezőit,
- a Tanúsítvány felépítését,
- az egyes mezők tartalmát,
- a Tanúsítványban alkalmazott névformátumokat,
- az ezekre vonatkozó kötöttségeket,
- az időbélyeg felépítését.

A 8. (HSzSz adminisztráció) fejezet ismerteti a szolgáltatást meghatározó kapcsolódó dokumentumok változatásának, elfogadtatásának és publikálásának szabályait.

A 9. (Hivatkozások és Meghatározások) fejezet a jelen szabályzatban hivatkozott jogszabályok, belső szabályzatok, szabványok és ajánlások, valamint a használt kifejezések értelmezését, magyarázatát tartalmazza.

1.1.3. Jogszabályok, szabványok

A jelen HSzSz a következő jogszabályokat, szabványokat, és ajánlásokat vesz figyelembe:

- a HSzSz teljes tartalmára 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,
- ISO/IEC 15408 1999: Információ technológia - Biztonsági módszerek - Informatikai biztonság értékelési kritériumai (1-3 részek)

♦ A HSzSz szerkezetére és tartalmára vonatkozóan:
- RFC 2527 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és szolgáltatási szabályzat keretrendszer)
- Európai Unió ETSI TS 101 456 szabvány,
- American Bar Association (ABA),
- PKI Assessment Guidelines (PAG),

♦ A minősített tanúsítványok, visszavonási listák szerkezete, tartalmára vonatkozóan:
- International Telecommunication Union X.509 "Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer"
- Minősített tanúsítványtípus minták minősített hitelesítés-szolgáltatók számára, 1.0 verzió. Hírközlési Felügyelet.
- ETSI TS 101 862 Minősített tanúsítvány profil
- RFC 2459 (Internet X.509 Nyilvános kulcsú infrastruktúra – Tanúsítvány és Tanúsítvány visszavonási lista profil)
- ITU-T X.509 "Information technology - Open Systems Interconnection - The Directory: Public -key and attribute certificate frameworks" ajánlás 3. verziója,
- RFC 3039 (Internet X.509 Nyilvános kulcsú infrastruktúra – Minősített tanúsítvány profil)
- ISO 3166

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

- 2/2002. (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről,
- ETSI TS 101 456 (Minősített tanúsítványokat kibocsátó hitelesítés-szolgáltatókra vonatkozó szabályozási követelmények).

♦ Az időbélyegzésre vonatkozóan:
- RFC – 3161 (Internet X.509 nyilvános kulcsú infrastruktúra időbélyeg protokoll)
- ETSI TS 102 023 (2003.04) (Időbélyegzés szolgáltatókra vonatkozó követelmények)
- ETSI TS 101 861 szabvány (Időbélyegzés profil)

♦ Az informatikai biztonsági követelményekre vonatkozóan: MeH 12. ajánlás, ITSEC[1], CC[2]

♦ A kriptográfiai modulra, az Aláírás létrehozó eszközre vonatkozóan:
- NIST FIPS PUB 140-1 (1994. január 11.) (Kriptográfiai modulok biztonsági követelményei),
- ITSEC,
- CC,
- 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. HSzSz azonosítás

A Szolgáltató 2003. január 31.-én beadta kérelmét a minősített szolgáltatás megindítására és a hatályos jogszabály által előírt dokumentumokat a Hírközlési Felügyeletnek átadta.

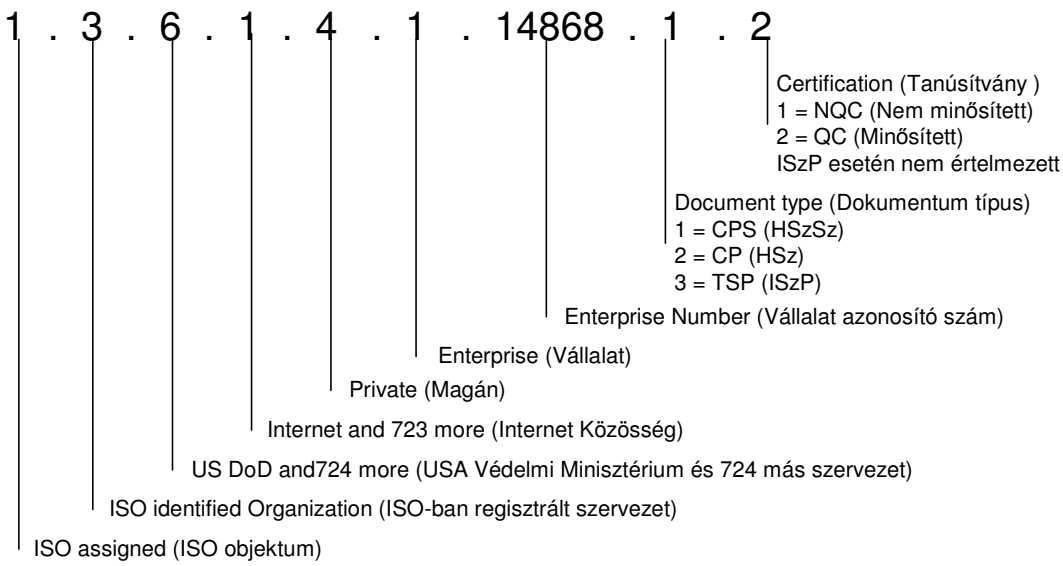
[1] ITSEC = Information Technology Security Evaluation Criteria (Információtechnológia Biztonsági Értékelési Kritériumok) az Európai Közösség ajánlása az IT termékek és rendszerek biztonságának funkcionális és minősítési követelményeire.

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

A Hírközlési Felügyelet a hatályos jogszabály által előírt minősítési eljárásokat lefolytatta és 2003. április 3.-án a Szolgáltatót minősített elektronikus aláírás hitelesítés szolgáltatóként nyilvántartásba vette (nyilvántartási adatokat ld 1.5 pont).

A Szolgáltató az ISO/IEC és az ITU szabványok által előírt regisztrációs eljárásnak megfelelően eljárva azonosítja a jelen HSzSz-t.

OID szám:



1. ábra Nemzetközi azonosító

A szabályzat a következő tanúsítványtípus kezelését írja le:

Nyilvános körben kibocsátott minősített tanúsítványtípus (**MTT**)

OID: 1.3.6.1.4.1.14868.2.2.1

Hírközlési Felügyelet azonosító: MH-2460-8/2003.

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

OID: 1.3.6.1.4.1.14868.2.2.2

Hírközlési Felügyelet azonosító: MH-2460-8/2003.

A szabályzat vonatkozó pontjai tartalmazzák az időbélyegzés szolgáltatásra vonatkozó gyakorlati szabályokat és megoldásokat, amelyek a MÁV INFORMATIKA Kft. Időbélyegzés

Szolgáltatási Politikája (továbbiakban: ISzP) (OID: 1.3.6.1.4.1.14868.3) szerint lettek kialakítva.

Jelen dokumentum teljes neve:

Trust&Sign® Hitelesítés Szolgáltatási Szabályzat Minősített Elektronikus Aláírással Kapcsolatos Szolgáltatásokra.

A jelen dokumentumban HSzSz-ként történik rá hivatkozás.

A HSzSz az Interneten a következő címeken keresztül érhető el:
„http://www.mavinformatika.hu/ca/**”.**

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

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.

Időbélyegzés vonatkozásában a közösséget az ISzP 4. pontjában meghatározott, következő csoportok alkotják:

- időbélyegzés szolgáltató (továbbiakban: ISz),
- időbélyeg felhasználó (igénybevevő) fél,
- érintett fél.

Az időbélyegzés szolgáltatást minden, az ISzP 4.3 pontban meghatározott szerződéses fél igénybe veheti, függetlenül attól, hogy az időbélyeget nyilvános vagy zárt körben használja.

A MÁV INFORMATIKA Kft. PKI Üzleti Egysége nyújtja az időbélyegzés szolgáltatást.

1.3.1. Hitelesítési Politika és Szabályozási Csoport

A Hitelesítési Politika és Szabályozási Csoport a Szolgáltató által létrehozott szervezeti egység, amely a szolgáltatással kapcsolatos politikák és szabályzatok kialakításáért, elfogadásáért, karbantartásáért és adminisztrációjáért felelős. A Regisztrációs Irodák (ld. 1.3.3 pont) és az Ügyfélkapcsolati Irodák (ld. 1.3.4 pont) által létrehozott szabályokat a Hitelesítési Politika és Szabályozási Csoport ellenőrzi a Szolgáltató szabályzatainak, szerződésének és üzletpolitikájának való megfelelőség szempontjából.

A Hitelesítés Politika és Szabályozási Csoport a MÁV INFORMATIKA Kft. Biztonsági Osztálya alá van rendelve.

1.3.2. Hitelesítő Központ

A hitelesítés és az időbélyegzési politikákban meghatározott hitelesítő és időbélyegző szervezetet a Szolgáltató Trust&Sign® Hitelesítő Központja testesíti meg.

A Hitelesítő Központ a Szolgáltató központi eleme, amely a szolgáltatás-támogató informatikai rendszer központi erőforrásaiból, azt ezt körül vevő biztonságos fizikai környezetből (Bizalmi Központból, ld. 5.1.1 pont), valamint az üzemeltető és szolgáltatást ellátó személyzetből áll. Feladata a különböző osztályú és típusú aláírás létrehozó adatok és tanúsítványok előállítása, ezek nyilvános publikálása, a Ügyfélkapcsolati Irodáktól (ld. 1.3.4 pont) érkező módosítási, felfüggesztési, újra aktivizálási, visszavonási és megszüntetési igények jelen HSzSz szerinti végrehajtása, az időbélyegzési kérelmek fogadása és kiszolgálása és a szolgáltatás támogató informatikai rendszer működtetése és menedzselése.

A Szolgáltató a fizikailag létező Trust&Sign® Hitelesítő Központjában működtet és menedzsel egy „Root CA” központot, amely a „Produktív CA”-k számára biztonságosan előállítja és kriptográfiai modulban biztonságosan tárolja a „Produktív CA”-k minősített tanúsítvány aláíró, infrastrukturális és rendszervezérlési kulcsait.

A Produktív CA-k fő feladata a Regisztrációs Iroda igényei alapján az előfizetők számára a kulcspárok generálása, a kapcsolódó tanúsítvány előállítása és ezek eljuttatása a Regisztráció Irodához. A „root CA” és a „produktív CA” feladatait részletesen a 2.1.2 pont ismerteti.

Az időbélyegzés szolgáltatást támogató kettőzött szerverek a szolgáltató Bizalmi Központjában üzemelő hitelesítés szolgáltató rendszerbe lettek beintegrálva, így azzal közösen állnak a tűzfalak védelme és a nagy megbízhatóságú rendszervezérlést végző szoftver irányítása alatt.

A szerverek belső óráját egy nála pontosabb másik belső óra szinkronizálja, amelyet négy egymástól független UTC külső időforrásból származó időjel szinkronizálja. Az időbélyegző szerver pontossága folyamatos ellenőrzés alatt áll. A külső UTC idők hitelességét egy erre a célra alakított bizottság hitelesíti az időbélyegző rendszer indításakor, illetve üzem közben, ha a hitelességgel kapcsolatban kétely merül fel. Ilyenkor referenciaként egy GSM kapcsolaton keresztül lekérdezett UTC idő szolgál.

Az ISz időbélyeg aláíró kulcspárját az időbélyegző egységben elhelyezett HSM generálja és tárolja. Az aláíró kulcs tanúsítványát a „root CA" írja alá.

Az időbélyegző központ által megvalósított feladatokat részletesen a 2.1.2 pont ismerteti.

A Trust&Sign® Hitelesítő Központ a következő alegységekből áll:

- a Szolgáltató minősített „Root CA" hitelesítő egysége (önhitelesített),
- a Szolgáltató minősített felhasználói „Produktív CA" hitelesítő egysége (root által hitelesített),
- időbélyegző egység,
- működtetési és menedzselési munkahelyek.

A Szolgáltatónál a Hitelesítő Központhoz kapcsolódó feladat-, felelősség- és hatásköröket a PKI Üzleti Egység gyakorolja.

1.3.3. Regisztrációs Iroda

A hitelesítés politikákban meghatározott regisztráló szervezet a Szolgáltatónál a következő szervezeti egységekből áll:

- Regisztrációs Iroda (perszonalizációs munkahelyek; rövidítve „RA"-k),
- Ügyfélkapcsolati Irodák, amelyek közül egy a Szolgáltató központi épületében működik.

A Regisztrációs Iroda a szolgáltatás keretein belül biztosítja az előfizetők technikai regisztrációját, a tanúsítványok felfüggesztés és visszavonás kezelését és az Aláírás-létrehozó eszközön az Aláírás-létrehozó adat elhelyezését. Egyúttal közreműködik további elektronikus alá-

írással kapcsolatos szolgáltatások biztosításában: tanúsítvány előállítás, kibocsátás és visszavonási állapot közzététele.
A Trust&Sign® Regisztrációs Irodákhoz kapcsolódó feladat-, felelősség- és hatásköröket a PKI Üzleti Egység gyakorolja.

Az időbélyegzés szolgáltatásban a Regisztrációs Iroda nem lát el faladatokat.

1.3.4. Ügyfélkapcsolati Irodák

Az Ügyfélkapcsolati Irodák a Szolgáltató és a vele szerződéses alapon együtt működő Társaságok (mint szerződött közreműködők) azon szervezeti egységei, amelyek az előfizetők adatainak regisztrációját, ellenőrzését, az igénylő személyazonosságának és hitelességének megállapítását, a tanúsítvány kérelmek összeállítását, a Hitelesítő Központ Regisztrációs Iroda (RA) alegységéhez történő továbbítását, és egyéb azonosítási, tanúsítványmenedzsment és adminisztrációs feladatokat látnak el.

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

Az Ügyfélkapcsolati Irodák az időbélyegzés szolgáltatás keretében elvégzi a leendő előfizetők egyszerűsített azonosítás-hitelestését, a szerződéskötést, az időbélyegzés szolgáltatást igénybevevő személyek nyilvántartását, és a nyújtott szolgál elszámolását. Az Ügyfélkapcsolati Iroda feladatai részletesen a 2.1.5 pont ismerteti.

Az Ügyfélkapcsolati Irodák szervezetileg a PKI Üzleti Egységhez tartoznak.

Az Ügyfélkapcsolati Irodák elérhetősége a „http://www.mavinformatika.hu/ca/” weboldalon található.

1.3.5. Végfelhasználók

1.3.5.1. Előfizető

Előfizető a Szolgáltatóval, az Általános Szolgáltatási Feltételekben foglaltak szerint szerződéses viszonyban álló felhasználó, aki számára a Szolgáltató Tanúsítványt és/vagy időbélyeget bocsát ki. Előfizető lehet természetes, illetve jogi személy.

Az Előfizető lehet egyben Aláíró is, amennyiben saját maga birtokolja és használja az Aláírás létrehozó adatot.

Az Előfizető lehet jogi személy (szervezet) is. Ebben az esetben aláíró képviselőjeként és/vagy időbélyeg igénylőként egy természetes személyt bíz meg, akit felruház a szolgáltatások igénybevételével. Ez a személy a jogi személyt képviselve ír alá vagy kér időbélyeget.

Tehát Aláíró és/vagy időbélyeg igénylő lehet:

a) bármely magyar állampolgárságú természetes személy, aki személyazonosságát a regisztráció során a HSzSz 3.1.8 pontjában előírtak szerint igazolta.

b) bármely természetes személy, aki részére Tanúsítvány és/vagy időbélyeg azzal a céllal kerül kibocsátásra, hogy az Aláírót és/vagy az időbélyeg kérő felet más természetes vagy jogi személy (szervezet) képviseletében történő aláírásra és/vagy időbélyeg kérésre jogosítsa fel. Ebben az esetben a személyazonosság ellenőrzése mellett a regisztráció során a 3.1.8 pontban meghatározott módon a képviseleti jogosultságot is ellenőrizni kell.

Igénylő lehet bármely természetes személy vagy jogi személy képviselője, aki a Szolgáltató szolgáltatásai iránt érdeklődik. Az igénylői státusz a szerződéskötés lezárásáig tart. Sikeres szerződéskötés után az Igénylő Előfizetővé válik, illetve Aláíróvá és/vagy időbélyeg kérő féllé is, amennyiben az Előfizető és az Aláíró és/vagy az időbélyeg kérő fél ugyanazon természetes személy.

1.3.5.2. Érintett fél

Az Érintett fél olyan természetes vagy jogi személy, aki vagy amely az aláírt és/vagy időbélyegzett elektronikus dokumentum fogadója, és egy adott Tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el az aláírás és/vagy az időbélyeg hitelességének ellenőrzésekor.

1.3.6. Alkalmazhatóság

1.3.6.1. Szabályzat hatálya

A HSzSz időbeli hatálya

A HSzSz 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 lépésekor.

A HSzSz személyi hatálya

Az 1.3 pontban meghatározott hitelesítés és időbélyegzés szolgáltató és felhasználói közösségre terjed ki.

A HSzSz tárgyi hatálya

A következőkre terjed ki:

- az 1. pontban meghatározott szolgáltatásokra,
- a Szolgáltatónak a Trust&Sign® hitelesítés és időbélyegzés szolgáltatással valamilyen kapcsolatban álló összes objektumaira, tárgyi eszközeire.

1.3.6.2. Szolgáltatás szintje

A Szolgáltató a 2001. évi XXXV. sz. elektronikus aláírásról szóló törvény szerinti minősített szolgáltatást nyújt az 1. pont szerint. A Trust&Sign® szolgáltatások az alábbi összetevőkből épülnek fel:

- Tanúsítvány kialakítási szolgáltatás, ebben regisztráló szolgáltatás és egyedi-név szolgáltatás, valamint megszemélyesítési szolgáltatás;
- Tanúsítvány előállítás és tanúsítvány szétosztási szolgáltatás;
- Felfüggesztési és visszavonás kezelési szolgáltatás;
- Tanúsítvány archiválási és állapotinformációs szolgáltatás, valamint adattárolási szolgáltatás;
- Tanúsítvány megújítási szolgáltatás;
- Biztonságos aláírás-létrehozó eszköz fizikai megszemélyesítése (szolgáltató arculati elemeinek elhelyezése az eszközön);

- Biztonságos aláírás-létrehozó eszköz logikai megszemélyesítése (tanúsítványok és magánkulcs[3] elhelyezése eszközön);
- Időbélyegzés szolgáltatás.

A Szolgáltató a minősített szolgáltatást támogató eszközeit a 16/2001. (IX.1.) MeHVM rendelet 24.§ (1) bekezdésnek megfelelően a fokozott biztonságú, illetve a teszt célú szolgáltatásokat támogató eszközeitől elválasztva használja és üzemelteti az 5.1 fejezetben ismertetett Bizalmi Központban.

A Szolgáltatás megfelelőségét a 2.7 pont alapján auditor tanúsítja.

1.3.6.3. Tanúsítványok alkalmazhatósága

A Trust&Sign® tanúsítványok alkalmazhatóságára a következő alapszabályok érvényesek:

1. Engedélyezett alkalmazási lehetőségek
2. A kibocsátott magánkulcsok elektronikus dokumentumon elektronikus aláírások megtételére. A nyilvános kulcsok (amelybe egyéb célú nyilvános kulcsok nem értendők bele) a tanúsítványok aláírásának ellenőrzésére használhatók fel, a Tanúsítványba foglaltaknak megfelelően. Korlátozott alkalmazási lehetőségek

   Szolgáltató általi területi, pénzügyi, stb. korlátozásokat szabhat saját belső hitelesítési politikája (HP) szerint, amelyeket a kibocsátott Trust&Sign® Tanúsítványban megad.

   Egyébként a Szolgáltató nem korlátozza a kibocsátott tanúsítványok felhasználhatóságát. Az Előfizető szervezet élhet korlátozásokkal Aláíró és érintett felek tanúsítvány felhasználási tevékenységével kapcsolatosan.
3. Tiltott alkalmazási lehetőségek

   A Trust&Sign® előfizetői tanúsítványok más nyilvános kulcsú tanúsítványok aláírására történő felhasználása, vagy bármilyen hitelesítés szolgáltatás nyújtásához történő alkalmazása tilos.

A fentiek alapján a kibocsátott Trust&Sign® Tanúsítványok (illetve az ezekhez kapcsolódó kulcspár) felhasználhatók minden olyan számítástechnikai alkalmazásban, amely támogatja a

[3] A jogszabályok ezt a szolgáltatást „aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezése” néven nevezik.

PKI technológián alapuló elektronikus aláírási, azonosítás-hitelesítési, le nem tagadhatósági funkciókat. Amennyiben a Szolgáltató elektronikus aláírás hitelesítés céljából bocsát ki Tanúsítványt, 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.

A 2/2002. (IV.26) MeHVM irányelve 214. pontja értelmében az időbélyegzéshez használt aláíró kulcsokat kizárólag a Szolgáltató által létrehozott időbélyegzők aláírására lehet használni. A Szolgáltató ennek megfelelően jár el.

Jelen HSzSz hatálya alatt kibocsátott tanúsítványok csak az 1.3 fejezetben meghatározott hitelesítés-szolgáltató és felhasználó közösség körében használhatók az ÁSzF-ben, illetve az Előfizetői Szerződésben meghatározott összeghatárok szerinti korlátokkal.

A Trust&Sign® Tanúsítvány használati lehetőségére vonatkozó 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. Tanúsítványok osztály, tanúsítványtípus és tanúsítvány fajta

A jelen HSzSz csak a nyilvános körben kibocsátott Trust&Sign® minősített tanúsítványokat és az ezzel kapcsolatos szabályokat írja le.

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

- fokozott biztonságú,
- minősített,
- teszt

tanúsítványok osztálya.

A jelen HSzSz csak a minősített tanúsítványokra vonatkozik.

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 felhasználás területe és célja szerint:

- előfizetői
- szolgáltatói

használati osztályokat különböztetünk meg.

A Szolgáltató kötelezettség vállalása egyszintű, amelynek mértéke a Trust&Sign® Tanúsítvány típusától és fajtájától függően kerül meghatározásra. A kötelezettség vállalás értékhatárát az Előfizetői Szerződés rögzíti és ez az értékhatár a Tanúsítványban (7.1.2 pont) is szerepel.

A Szolgáltató felelősség vállalásának mértékét 2.2.1 és a 2.3.1 pontok határozzák meg.

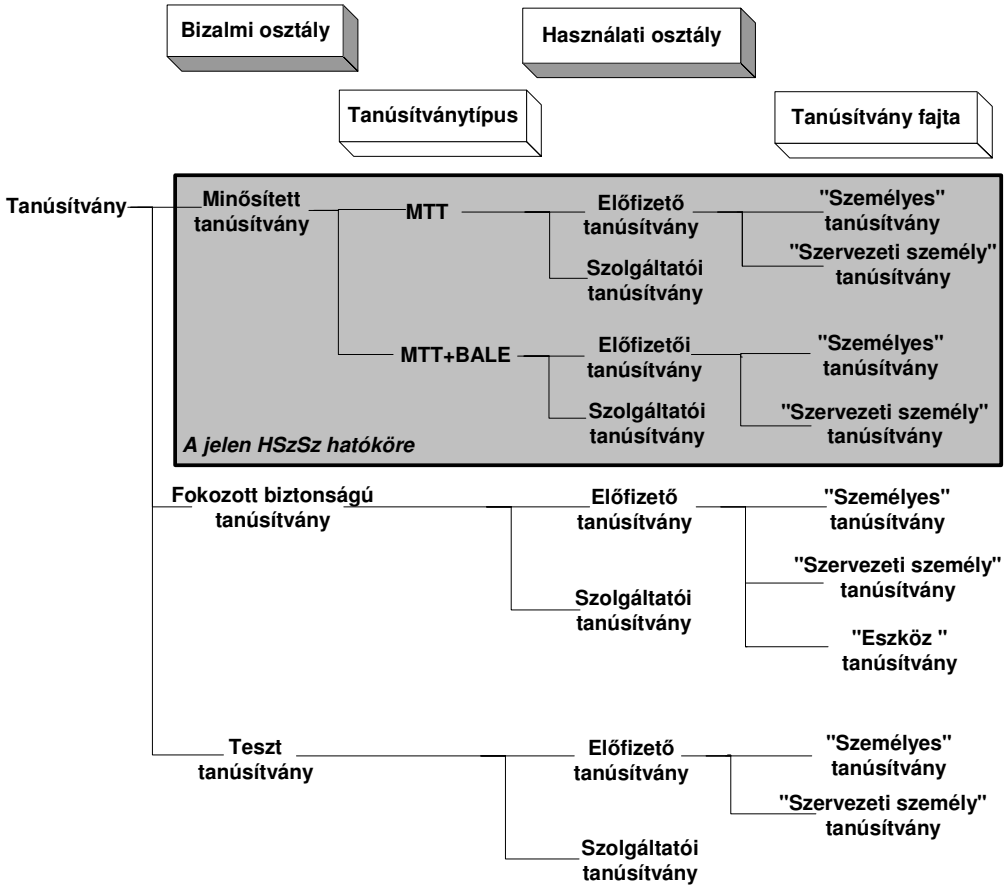
A 2. ábra mutatja a tanúsítvány osztályok hierarchiáját.

A szürke színnel jelzett terület foglalja magában a minősített tanúsítványok osztályába tartozó MTT és az MTT+BALE tanúsítványtípusokat. A jelen HSzSz csak ezekre a típusokra vonatkozik.

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

A jelen HSzSz a következő tanúsítvány fajtákat különbözteti meg:

- „személyes” tanúsítvány,
- „szervezeti személy” tanúsítvány.



2. ábra. Tanúsítvány osztályok, típusok és fajták

A minősített tanúsítvány osztály típusainak és fajtáinak jellemzőit az 1.4.1 és 1.4.3 pontok írják le.

1.4.1. Minősített tanúsítvány osztály jellemzői és típusai

1.4.1.1. Minősített tanúsítványok jellemzői

Minősített tanúsítvány az elektronikus aláírási 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, ennek jelzésével;

4. a Szolgáltató által menedzselt álnév formátum: ~álnév~
5. az Aláírónak külön jogszabályban, illetve a szolgáltatási szabályzatban, illetőleg az ÁSzF-ben meghatározott speciális jellemzőit, a Tanúsítvány szándékolt felhasználásától függően,
6. azt az Aláírás-ellenőrző adatot, amely az aláíró által birtokolt aláírást készítő adatnak felel meg,
7. a Tanúsítvány érvényességi idejének kezdetét és végét,
8. a Tanúsítvány azonosító kódját,
9. az adott minősített tanúsítványt kibocsátó Szolgáltató fokozott biztonságú elektronikus aláírását,
10. a Tanúsítvány használhatósági körére vonatkozó esetleges korlátozásokat,
11. a Tanúsítvány felhasználásának korlátjait, (beleértve a kötelezettségvállalás korlátait is)
12. más személy (szervezet) képviseletére jogosító elektronikus aláírás Tanúsítványa esetén a Tanúsítvány ezen minőségét és a képviselt személy (szervezet) adatait.

A minősített tanúsítványoknak két típusát különböztetjük meg.

1.4.1.2. Nyilvános körben kibocsátott minősített tanúsítványtípus (MTT)

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.

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

1.4.1.3. Nyilvános körben kibocsátott és Biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített tanúsítványtípus (MTT+BALE)

Az MTT+BALE olyan tanúsítványtípus, amely:

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

- 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,
- olyan Biztonságos aláíró eszköz került felhasználásra, amely eleget tesz a 2001. évi XXXV. törvény 1. számú mellékletében meghatározott követelményeknek,
- nyilvános körben került kibocsátásra.

Ezen alapkövetelmények alapján kibocsátott minősített tanúsítványok olyan elektronikus aláírások igazolására használhatók, amelyek az aláírás jogi követelményeit az elektronikus formájú adatok vonatkozásában ugyanolyan módon kielégítik, ahogy egy kézírásos aláírás kielégíti ugyanazt a követelményt a papír-alapú adatok vonatkozásában. Az ilyen aláírást minősített elektronikus aláírásnak kell tekinteni, amely olyan - fokozott biztonságú - elektronikus aláírás, amely Biztonságos aláírás-létrehozó eszközzel (BALE) készült, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.

1.4.2. 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.

Előfizetői tanúsítvány csak felelősségvállalással bocsátható ki, amelynek értékét az ÁSzF vagy az Előfizetővel történt megállapodás határozza meg.

Trust&Sign® 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	Az Aláíró a személyi igazolványával vagy az útlevélével személyesen igazolja

	magát. Cégszerűen aláírt képviseleti megbízás. Cégbíróságnál nyilvántartott gazdasági társaság esetén: 30 napnál nem régebbi cégkivonat, aláírási címpéldány. Nem cégbíróságnál nyilvántartott szervezetek esetében: a nyilvántartó szervezet igazolása. Állam-, illetve közigazgatási szervezetek esetében: az alapító dokumentum közjegyzővel hitelesített másolata, amelyet a szervezet első számú vezetőjének írásos nyilatkozatával együtt.

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 kell elvégezni.

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 típusú tanúsítványokat magyar állampolgárságú természetes személy igényelhet a saját nevében.

Az Előfizető és az Aláíró ugyanaz a személy.

Az Ügyfélkapcsolati Irodán 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.

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

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.

Az Ügyfélkapcsolati Irodán 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) 457-9300
Telefax szám:	(36-1) 457-9500
Internet cím:	http://www.mavinformatika.hu

Panaszok bejelentésének helye:

- Személyesen az Ügyfélkapcsolati Irodán
- írásban a Szolgáltató telephelyére címezve
- telefonon és faxon az Ügyfélkapcsolati Irodán vagy az Ügyfélszolgálatnál
- elektronikus levélben a Szolgáltató Internet 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

Kapcsolat az ügyfelekkel:

A vevői kapcsolatok (általános és részletes tájékozódás, szerződéskötés, aláírás létrehozó eszköz átadása, visszavonási kérelem megerősítése, stb.) biztosítása érdekében a Szolgáltató Ügyfélkapcsolati Irodát tart fenn, melyet az ügyfelek személyesen munkanapokon 9 és 13 óra között kereshetnek fel.

Az Ügyfélkapcsolati Iroda címe: Budapest, I. Krisztina krt. 37/a.

Az Ügyfélkapcsolati Iroda munkaidőben elérhető telefonon a +36-1-457-95-78 előfizetői közvetlen számon, vagy a +36-1-457-93-00 központi számon, valamint elektronikus levélben az ica@mavinformatika.hu címen.

A szolgáltatással kapcsolatban felmerült kérdések megválaszolására, valamint a Trust&Sign® Tanúsítványok felfüggesztésére, illetve visszavonási igény sürgős bejelentésére a Szolgáltató folyamatos (7x24 órás) ügyfélszolgálatot (Help Desk szolgálatot) ad.

Az Ügyfélszolgálat elérhető +36 80 39-93-93-as zöldszámon, a +36-1-457-93-93 közvetlen számon, a +36-1-457-93-00 központi számon, valamint elektronikus levélben a helpdesk@mavinformatika.hu címen.

Szolgáltató Ügyfélkapcsolati Irodája és Ügyfélszolgálata ügyfélszolgálati naplót vezet, amelyben minden megkeresésről a következő információkat rögzíti:

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

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

1.5.2. 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 +36-1-457-93-75 közvetlen vagy 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, a hitelesítési és az időbélyegzési politikákban, az ÁSzF-ben, az Előfizetői Szerződésekben és a Biztonsági Szabályzatban meghatározottak szerint jár el az előfizetők tanúsítványainak és időbélyegeinek kiadásakor és kezelésekor, amelynek keretében kötelezettséget vállal az alábbiakra:

1. A Szolgáltató (a Hitelesítő Központ, a Regisztrációs Iroda, az Ügyfélkapcsolati Iroda és az Ügyfélszolgálat együttes tevékenységével) az 1. és az 1.3.6.2 pontokban megjelölt szolgáltatásokat biztosítja;

   a szolgáltatások megnevezése: Trust&Sign®.
2. A Szolgáltató gondoskodik a Szolgáltatóra és a szolgáltatásra vonatkozó valamennyi, a jelen HSzSz 3.-8. pontjaiban részletezett állítások 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 az 1. pontban megjelölt szolgáltatásait a HSzSz szerint nyújtja.
7. A HSzSz-t a Szolgáltató vezetése hagyja jóvá; a HSzSz megfelelő megvalósításáért a Szolgáltató vezetése felel.
8. A Szolgáltató rendszeresen felülvizsgálja HSzSz-ét, az újra érvényesített szabályzat tartalmazza a szükséges módosításokat.

9. A Szolgáltató időben értesítést tesz közzé a szolgáltatási szabályzatában tervezett változtatásokról és a fenti (a 7. pont szerint történő) jóváhagyást követően az átdolgozott szolgáltatási szabályzatát (ezen felsorolás 15. pontjában előírtak szerint) haladéktalanul hozzáférhetővé teszi.
10. 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.
11. 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.
12. 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.
13. A Szolgáltató kötelezettséget vállal arra, hogy a tanúsítványigénylésnek a HSzSz-ben rögzítetteknek megfelelően történő elbírálását követően a lehető legrövidebb időn, de legkésőbb 30 munkanapon belül a Tanúsítvány, illetve az időbélyeg szolgáltatás igénylés feldolgozásáról intézkedik és a Tanúsítvány kibocsátásáról, illetve az időbélyeg szolgáltatás megkezdéséről az Előfizetőt az Ügyfélkapcsolati Iroda e-mail-ben értesíti. Jogi személy képviseletére jogosító Tanúsítvány esetén az értesítés a szervezet által meghatalmazott képviselőn keresztül történik. A Szolgáltató emellett nyilvántartást vezet a szolgáltatás kérelmek státusának állásáról, melyet a HSzSz-ben meghatározott módon tesz hozzáférhetővé az Ügyfélkapcsolati Iroda részére.
14. A Szolgáltató a szolgáltatások működtetése és menedzselése során a HSzSz-ben, az ÁSzF-ben, illetve az Előfizetői Szerződésben rögzített ügyfélkapcsolati tevékenységet az Ügyfélkapcsolati Iroda által biztosítja, amely egy műszakban fogadja az igénylőket, megadja a szükséges tájékoztatást és információkat, szerződést köt, átadja a Biztonságos aláírás létrehozó eszközöket, fogadja a tanúsítvány visszavonási igényeket.

A Szolgáltató az Ügyfélszolgálata (Help Desk szolgáltatása) keretében folyamatos (7x24 órás) felügyeletet biztosít az előfizetői kérdések, panaszok és felfüggesztési igények kezelésére.

15. A Szolgáltató vezeti és közzéteszi a jogszabály szerinti nyilvántartásokat, valamint a Tanúsítvány, illetve időbélyeg kibocsátására vonatkozó saját szabályzatait (HSzSz, HP-k, ISzP, ÁSzF), Internet segítségével, bárki számára folyamatosan[5] elérhető módon.

16. A Szolgáltató értesítést küld e-mail-ben a lejáró Tanúsítványokról az Előfizető és az Aláíró részére legalább 15 nappal a lejárat előtt, és kéri az Előfizető, illetve az Aláíró további intézkedését a tanúsítvánnyal kapcsolatban. Az e-mail értesítés 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.

17. Szolgáltató a Tanúsítvány megfelelő mezőjében feltünteti, ha az ÁSzF, illetve az Előfizetői Szerződés a Tanúsítvány felhasználhatóságával kapcsolatban megjelenő összeg, területi vagy egyéb korlátozásokat.

18. A Szolgáltató felfüggeszti a Tanúsítvány érvényességét és ezt nyilvánosan elérhető helyen közzéteszi a http://www.mavinformatika.hu/ca/**,** vagy a **http://crl.trust-sign.hu** web lapon keresztül, amennyiben:

    18.1. az Előfizető vagy az Aláíró ezt az ÁSzF-ben meghatározott módon kéri,

    18.2. a szolgáltatásokkal kapcsolatos – jogszabályban meghatározott – rendellenességről szerez tudomást,

    18.3. megalapozottan feltételezhető, hogy a Tanúsítványban foglalt adatok nem felelnek meg a valóságnak, vagy az Aláírás létrehozó adat nem az Aláíró kizárólagos birtokában van,

    18.4. a Hírközlési Felügyelet jogerős és végrehajtható határozatában így rendelkezik.

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

19. A Szolgáltató köteles a Tanúsítvány visszavonására és ennek közzétételére az alábbi esetekben:
    19.1. 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,
    19.2. amennyiben a képviseleti jogosultság megszűnéséről a képviselt természetes vagy jogi személy illetve a képviselő (Aláíró) a Szolgáltatónak bejelentést tesz,
    19.3. amennyiben a Szolgáltató a szolgáltatással kapcsolatos – jogszabályban, HSzSz-ben meghatározott – rendellenességről vesz tudomást és a rendellenesség az ezen dokumentumokban meghatározott szabályok szerint nem orvosolható,
    19.4. amennyiben tudomására jut, hogy a Tanúsítványban foglalt adatok nem felelnek meg a valóságnak, vagy az Aláírás létrehozó adat nem az aláíró kizárólagos birtokában van,
    19.5. a Szolgáltató és az Előfizető között a szerződés megszűnt,
    19.6. a Felügyelet jogerős és végrehajtható határozatában így rendelkezik,
    19.7. a Szolgáltató a tevékenységét befejezte,
20. A Szolgáltató kötelezettséget vállal arra, hogy a részére beadott visszavonási kérelmeket a HSzSz-ben meghatározott feltételek szerint feldolgozza, és a visszavont Tanúsítványok a visszavonási listákon közzétételre kerülnek.
21. A Tanúsítványok lejárat előtti visszavonásának jogkövetkezményei az alábbiak:
    21.1. a visszavont Tanúsítvány a továbbiakban a jelen HSzSz 1.3.6.3 pontjában meghatározott tevékenységek végzésére nem használható. Ha az Aláíró az Aláírás létrehozó adatot felhasználja, az aláírás ellenőrzője jogosult az elfogadás megtagadására,
    21.2. a visszavonást követően nem kerül automatikusan új Tanúsítvány kibocsátásra;

    Azt az új Tanúsítványok igénylésével azonos igénylési folyamatnak kell megelőznie.
22. Szolgáltató megőrzi a szolgáltatással kapcsolatos elektronikus információkat és az ahhoz kapcsolódó személyes adatokat legalább a Tanúsítvány érvényességének lejáratától szár-

mazó 10 évig; továbbá – amennyiben ezen időszakban az elektronikus aláírással, az azzal aláírt elektronikus dokumentummal vagy az időbélyegzéssel 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.

23. 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.
24. A Szolgáltató az időbélyegzés szolgáltatás vonatkozásában kötelezettséget vállal a következőkre:
    24.1. az időbélyegben megadott időpont az ISzP-ben meghatározott 1 másodperces pontosságú;

    amennyiben az időbélyegző szerver órája túllépné az előírt pontossági határt, akkor az időbélyegzés szolgáltatást a rendszer leállítja, és hibaüzenetben értesíti az előfizetőket erről,

    24.2. az időbélyegzés szolgáltatást 99,5%-os rendelkezésre állással biztosítja,

    24.3. az időbélyegző rendszer időszinkronizációját 0,1 másodperc pontossággal és magas megbízhatósági szinten (háromszoros tartalékolással) biztosítja,

    24.4. a szinkronozást biztosító külső UTC időalapok hitelességét a rendszer indításakor egy erre a célra alapított bizottság tanúsítja;

    amennyiben felmerül a gyanú, hogy a hitelesség sérül, akkor a bizottság összehívásra kerül, ellenőrzi a UTC idők hitelességét, amelyhez referenciaként egy független GSM kapcsolaton keresztül lekérdezett UTC időt használ,

    24.5. biztosítja, hogy a Szolgáltató időbélyeg aláíró kulcsa fokozottan biztonságos körülmények között generálódik és tárolódik a 2/2002. (IV.26) MeHVM irányelvben előírt tanúsítással rendelkező HSM-ben,

    24.6. az időbélyeg kérő fél által küldött állományon a teljes időbélyegzési eljárás folyamán nem változtat, annak tartalmát nem ismeri meg és változatlan formában és tartalommal egy biztonságos csatornán visszaküldi.

25. Ha a Szolgáltató be kívánja fejezni tevékenységét, erről a tevékenység befejezését legalább hatvan nappal megelőzően értesítenie kell a szolgáltatások előfizetőit, az általa kibocsátott és még vissza nem vont Tanúsítványok aláíróit, az általuk képviselt természetes vagy jogi személyt, valamint a Hírközlési Felügyeletet, megjelölve a 25. bekezdés szerinti szervezetet. A bejelentés időpontjától kezdve a Szolgáltató nem bocsáthat ki új Tanúsítványt és időbélyeget. 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.
26. 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.
27. A Szolgáltató az Előfizetői Szerződésben rögzíti a szolgáltatások díjtételeit.

2.1.2. A Hitelesítő Központok („CA”-k) feladatai és hatásköre

A Szolgáltató által működtetett Hitelesítő Központok feladata és hatásköre általában az elektronikus aláírással kapcsolatos alábbi szolgáltatások megvalósítása:

- tanúsítvány előállítás;

  egyúttal közreműködik (a visszavonási listák aláírásával) a visszavonási állapot közzétételében,
- időbélyegzés.

A Hitelesítő Központok 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 előállítják a Tanúsítványt (aláírják a megadott 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 Regisztrációs Irodának a tőle kapott tanúsítvány kérelmet, benne elküldve az előállított Tanúsítványt, biztosítva a válaszüzenet sértetlenségét és hitelességét.

A Hitelesítő Központok a visszavonási állapot közzététele szolgáltatásban való közreműködés keretén belül:

1. ellenőrzik a Regisztrációs Irodától érkező visszavonási lista aláírási kérelmet, s ebben az aláírandó Tanúsítvány visszavonási lista sértetlenségét és hitelességét,
2. feldolgozzák a Regisztrációs Irodától 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 Regisztrációs Irodától kapott visszavonási lista aláírási kérelmet, elküldve az aláírt Tanúsítvány visszavonási listát, biztosítva a válaszüzenet sértetlenségét és hitelességét.

Az 1. szintű „Root CA” alapvető feladata és hatásköre a 2. szintű „Produktív CA” és az időbélyegző központ 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. Szolgáltató Hitelesítő Központok hitelesítési kérelmeinek fogadása és ellenőrzése.
6. Tanúsítvány előállítás Szolgáltató "Produktív CA" Hitelesítő Központok részére.
7. Tanúsítvány előállítása az időbélyegző központ részére.
8. Szolgáltató „CA" Tanúsítvány visszavonási kérelmeinek feldolgozása.
9. Szolgáltató Hitelesítő Központok Tanúsítvány megújítási kérelmeinek feldolgozása.
10. Tanúsítvány eljuttatása a Szolgáltató "Produktív CA" Hitelesítő Központhoz.
11. Szolgáltató Hitelesítő Központok Tanúsítványainak és visszavonási listáinak publikálása a címkönyvtárban.
12. Szolgáltató Hitelesítő Központ Tanúsítványának visszavonása, illetve felfüggesztése, amennyiben magánkulcsa kompromittálódik, vagy ennek gyanúja áll fenn.
13. Az általa tanúsított Hitelesítő Központok bizalmi és biztonsági ellenőrzése.

A 2. szintű „Produktív CA" Hitelesítő Központ alapvető feladat és hatásköre a Regisztrációs Iroda ("RA") és az általa ellenőrzött és regisztrált előfizetők hitelesítése, ezen belül a feladatok tételesen a következők:

1. Saját magánkulcs generálás.
2. A saját Magánkulcsának MeH 12. ajánlás szerinti fokozott biztonságú védelme.
3. A Regisztrációs Iroda hitelesítési kérelmeinek fogadása és ellenőrzése.
4. A Regisztrációs Iroda és az Ügyfélkapcsolati Iroda tájékoztatása a tanúsítványkérelmek státuszáról.
5. Kulcs-pár generálás és Tanúsítvány előállítás a Regisztrációs Irodák részére.
6. Kulcs-pár és Tanúsítvány eljuttatása a Regisztrációs Irodákhoz.
7. Regisztrációs Irodáktól előfizetői hitelesítési kérelmek fogadása és ellenőrzése.
8. Tanúsítvány előállítás az előfizetők részére.
9. Regisztrációs Irodától érkező tanúsítvány visszavonási, felfüggesztési és újraérvényesítési kérelmek feldolgozása.
10. Regisztrációs Irodától érkező tanúsítvány megújítási kérelmek feldolgozása.
11. Tanúsítványok és tanúsítvány visszavonási listák publikálása a Címtárban.
12. Intézkedni tanúsítványok visszavonása, illetve felfüggesztése végett, amennyiben magánkulcsa kompromittálódik, vagy ennek gyanúja áll fenn.

13. A folyamatos[6], biztosítása a tanúsítvány felfüggesztési és visszavonási kérelmek végrehajtása érdekében, 99,9%-os rendelkezésre állással.
14. A Regisztrációs Irodák bizalmi és biztonsági ellenőrzése.

Az időbélyegzés szolgáltatást a Bizalmi Központban a hitelesítés szolgáltató informatikai rendszerbe integrálva valósítják meg az időbélyegző alkalmazást futtató kettőzött szerverek, valamint, az időszinkronizálást, a naplózást, az UTC időkkel és a belső órákkal kapcsolatos funkciókat, valamint a magas rendelkezésre állással kapcsolatos feladatokat megvalósító különböző hardver és szoftver rendszerelemek. A továbbiakban ezek együttesét nevezzük időbélyegző központnak, amelynek feladatai a következők:

1. megbízható csatornán keresztül fogadja az időbélyegzési kérelmeket,
2. azonosítja és hitelesíti az időbélyeg kérőt, ellenőrzi a kérelem szabályosságát,
3. előállítja az időbélyeget, amennyiben a Szolgáltató rendszere a pontos időt biztosítani tudja,
4. biztonságos csatornán keresztül elküldi az időbélyeget a felhasználónak szabványos formában,
5. ellenőrzi az időbélyegző szerver belső órájának pontosságát;

   amennyiben az óra a pontossági határon kívülre kerül, az időbélyegző szolgáltatást leállítja, és hibaüzenetet küld az előfizetők felé,
6. az időbélyegző szerver belső órájának az ISzP-ben előírt pontosságú szinkronizációja hiteles külső UTC idő alapján történik,
7. a belső óra pontosságának folyamatos ellenőrzése,
8. az időbélyeg aláíró kulcs fokozott biztonságú előállítása és tárolása a 2/2002. (IV.26) MeHVM irányelvnek megfelelően,
9. az időbélyegzéssel kapcsolatos események rögzítése, naplózása és archiválása.

2.1.3. A Hitelesítési Politika és Szabályozási Csoport feladatai és hatásköre

A Hitelesítési Politika és Szabályozási Csoport a Szolgáltató a szolgáltatást nyújtó szervezeti egységtől függetlenül működik. Kötelessége a Szolgáltató és felhasználó Közösség igényeinek felmérése és folyamatos követése, ezek alapján a közösség működésére vonatkozó alap-

6 A hét 7 napján, a nap 24 órájában.

elvek, politikák lefektetése, s ebből levezetve a tagok tevékenységét részletesen szabályozó, az egész Szolgáltató szervezetre nézve közös szabályzatok, így a HSzSz, a HP-k, az ISzP, 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 szabályozással kapcsolatos igényeinek felmérése.
2. A Tanúsítvány és az időbélyegzési politikák[7] elkészítése és karbantartása.
3. A HSzSz, a HP-k, az ISzP, az ÁSzF, az Előfizetői Szerződések és a Biztonsági Szabályzat elkészítése és karbantartása.
4. A Tanúsítvány és az időbélyegzési politikák, valamint a HSzSz közötti összhang rendszeres ellenőrzése és karbantartása.
5. A szolgáltatást támogató informatikai rendszer PKI és időbélyegzés 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 Regisztrációs Iroda (RA) feladatai és hatásköre

A Regisztrációs Iroda biztosítja az alábbi elektronikus aláírással kapcsolatos szolgáltatásokat:

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

[7] Megfelel az RFC 2527 ajánlásban definiált Certificate Policy (CP) fogalmának

Egyúttal közreműködik az alábbi elektronikus aláírással kapcsolatos szolgáltatások biztosításában:

- tanúsítvány előállítás,
- kibocsátás
- visszavonási állapot közzététele

A Regisztrációs Iroda a regisztráció szolgáltatás keretén belül:

1. ellenőrzi a dokumentumok érvényességét, valódiságát valós idejű nyilvántartásokban is;
2. 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;
3. nyilvántartásba vesz minden, a tanúsítványok kiadásához kapcsolódó, a 4.1 pontban meghatározott információt,
4. megőrzi a 3. pontbeli nyilvántartásokat a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított tíz évig, illetőleg velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig,
5. 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,
6. korlátozás nélkül biztosítja az Aláíró számára a rá vonatkozó regisztrációs és egyéb információhoz történő hozzáférést (lásd 2.8.7).

A Regisztrációs Iroda a visszavonás kezelés szolgáltatás keretén belül:

1. ellenőrzi a tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmek hitelességét és érvényességét (lásd még 4.5.2 és 4.5.6), valamint szabályosságát (lásd még 4.5.3 és 4.5.7),
2. haladéktalanul, maximum a 4.5.4, illetve 4.5.7 pontban meghatározott időn belül végrehajtja a hiteles, érvényes és szabályos, tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket (vagyis a kérelmezett változást átvezeti a Címtár alapját képező tanúsítvány állapot adatbázisába),

3. visszautasítja (az ok megjelölésével) a nem hiteles, érvénytelen, vagy szabálytalan, tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket,
4. a visszavonási kérelem elfogadása után haladéktalanul, maximum a 4.5.4 pontban meghatározott időn belül intézkedik egy tanúsítvány visszavonásáról,
5. intézkedik saját Tanúsítványának visszavonása, illetve felfüggesztése végett, amennyiben magánkulcsa kompromittálódott, vagy ennek gyanúja áll fenn,
6. folyamatosan[8], 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 Regisztrációs Iroda az Aláírás-létrehozó eszközön az Aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül:

1. gondoskodik valamennyi általa, az Aláíró számára végrehajtott kulcs előállítás biztonságosságáról, az Aláíró magánkulcsának titkosságáról,
2. az Aláíró részére biztosított kulcspárt:
   - olyan kriptográfiai eszközzel állítja elő, amely hazai tanúsítvánnyal igazolt és egyben szerepel a Hírközlési Felügyelet által nyilvántartásba vett, tanúsított elektronikus aláírási termékek listáján is,
   - olyan algoritmus felhasználásával állítja elő, melyet a 2/2002. (IV.26) MeHVM irányelv 1. sz. melléklete az elfogadott kriptográfiai algoritmusok között megfelelő kulcs generáló algoritmusként ismer el,
   - 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,
3. Minősített tanúsítvánnyal (MTT) kísért, szoftveres úton történő Aláírás létrehozó adat generálás esetén biztonságos módon eljuttatja az Aláíró részére előállított kulcspárt az Aláírás-létrehozó eszközbe, egy a kriptográfiai alkalmazás és az aláírás létrehozó eszköz közötti olyan biztonságos útvonal kiépítésével, mely megfelelő kriptográfiai mechanizmusok felhasználásával forráshitelesítést, sértetlenséget és bizalmasságot biztosít,

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

4. Minősített tanúsítvánnyal (MTT+BALE) kísért, a Szolgáltató kezdeményezésére Biztonságos aláíró eszközön történő Aláírás létrehozó adat elállítása esetén az adat az eszközön jön létre és azt az eszköz megsemmisítéséig nem hagyja el,
5. biztonságos módon megsemmisíti az Aláíró részére előállított magánkulcs Aláírás-létrehozó eszközön kívüli összes példányát, miután az Aláíró részére előállított kulcspárt elhelyezte a Biztonságos aláírás-létrehozó eszközben,
6. gondoskodik az általa megszemélyesített Aláírás-létrehozó eszköznek az Ügyfélkapcsolati Irodához a PIN-kód eljuttatásától független és biztonságos továbbításáról,
7. ellenőrzi az Aláírás-létrehozó eszköz kezelését,
8. ellenőrzi, hogy a szolgáltatáshoz felhasznált Aláírás-létrehozó eszköz a Hírközlési Felügyelet által nyilvántartásba vett Aláírás-létrehozó eszköz-e,
9. a Biztonságos aláírás létrehozó eszköz előkészítését megfelelően biztonságos környezetben (lásd 5.1 pont) hajtja végre,
10. biztonságos módon előállítja a kezdeti aktivizáló adatot (PIN kódot), majd azt az Aláírás-létrehozó eszköztől elkülönítve eljuttatja az Ügyfélkapcsolati Irodához,
11. biztosítja, hogy alkalmazottai nem élhetnek vissza az Aláírás-létrehozó eszközzel,
12. biztosítja saját Aláírás létrehozó adatainak biztonságos használatát és tárolását.

A Regisztrációs Iroda a tanúsítvány előállítás szolgáltatásban való közreműködés keretén belül:

1. a Tanúsítvány kibocsátásához szükséges ellenőrzések és visszaigazolások sikeres befejeződése után a Hitelesítő Központ felé tanúsítvány kibocsátási kérelem üzenetet indít el,
2. feldolgozza a teljes, pontos, hiteles és teljesíthető tanúsítvány megújítási kérelmeket az alábbi módon:
   - tanúsítványfrissítés kérelme esetén az Aláíró korábbi Tanúsítványában szereplő érvényességi időt meghosszabbítja, a többi adat és kulcspár változatlan megtartása mellett,
   - tanúsítvány aktualizálás kérelme esetén nyilvántartásba veszi az Aláíró megváltozott új adatait, a korábbi Tanúsítvány visszavonja és a megváltozott adatokkal új Tanúsítványt állít elő,
   - tanúsítvány kulcscsere kérelme esetén a korábbi Tanúsítvány visszavonja, új kulcspárt generál és új Tanúsítványt állít elő,

3. biztosítja az aláírandó Tanúsítványt is tartalmazó tanúsítvány kérelem üzenet sértetlenségét, hitelességét és bizalmasságát.

A Regisztrációs Iroda a tanúsítvány kibocsátás szolgáltatásban való közreműködés keretén belül:

1. fogadja a Hitelesítő Központtól kapott új tanúsítványokat, valamint ellenőrzi ezek hitelességét és sértetlenségét,
2. kezdeményezi az új tanúsítványok[9] elküldését a címtárhoz, biztosítva a kérést tartalmazó üzenet hitelességét és sértetlenségét.

A Regisztrációs Iroda a visszavonási állapot közzététele szolgáltatásban való közreműködés keretén belül:

1. rendkívüli esetben[10] új Tanúsítvány visszavonási listát készít tanúsítvány állapot adatbázisából, mely tartalmazza a visszavonási lista lejáratának idejét is,
2. kéri a Hitelesítő Központtól az új Tanúsítvány visszavonási lista kibocsátását, (a visszavonási lista aláírási kérelemben), biztosítva az ezt tartalmazó üzenet hitelességét és sértetlenségét,
3. kezdeményezi az új Tanúsítvány visszavonási listának a közzétételét, biztosítva az ezt tartalmazó üzenet hitelességét és sértetlenségét.

2.1.5. Az Ügyfélkapcsolati Iroda feladatai és hatásköre

Az Ügyfélkapcsolati Iroda szolgáltatás igénylés esetén az Igénylők, az előfizetők és az érintett felek részére nyújtott ügyfélkapcsolati tevékenység regisztráció szolgáltatásán belül:

1. gondoskodik az Igénylő megfelelő azonosításáról, illetve arról, hogy a Tanúsítványt igénylő formanyomtatványok teljesek, pontosak és kellőképpen hitelesek legyenek;
2. ellenőrzi a 3.1 pontban és az ÁSzF-ben előírt adatszolgáltatási követelmények szerint megadott adatok alapján a szolgáltatást igénylő ügyfél (természetes, illetve szervezeti személy) személyazonosságát és a leendő Aláíró és/vagy időbélyeg kérő fél 3.1 pontban meghatározott jellemzőit;

[9] Amennyiben az Aláíró hozzájárult ehhez.

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

3. összegyűjti, illetve meghatározza a regisztráció során valamennyi, a 3.1 pontban 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,
6. nyilvántartásba vesz minden, a regisztráció során felvett, a 4.1 pontban meghatározott információt,
7. megőrzi a 6. pontbeli nyilvántartásokat a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított tíz évig, illetőleg velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig.

Az Ügyfélkapcsolati Iroda a visszavonás kezelés szolgáltatás keretén belül:

1. ellenőrzi a tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmek hitelességét és érvényességét (lásd még 4.5.2 és 4.5.6), valamint szabályosságát (lásd még 4.5.3 és 4.5.7),
2. tájékoztatja a visszavont, illetve felfüggesztett Tanúsítvány tulajdonosát Tanúsítványa állapotának változásáról.

Az Ügyfélkapcsolati Iroda az Aláírás-létrehozó eszközön az Aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül:

1. gondoskodik valamennyi általa, az Aláíró számára előállított Aláírás-létrehozó eszköz, az Aláírás-létrehozó adat és a PIN kód biztonságos kezeléséről és az Aláírónak történő biztonságos átadásukról,
2. biztosítja, hogy alkalmazottai nem élhetnek vissza az Aláírás-létrehozó eszközzel.

Az Ügyfélkapcsolati Iroda 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. az Aláíró adatainak változása, illetve kulcscsere kérelem esetén ellenőrzi a már korábban nyilvántartásba vett Aláírótól érkező tanúsítvány megújítási kérelem teljességét, pontos-

ságát, hitelességét és teljesíthetőségét a 3.1 pontban a kezdeti regisztrációnál meghatározott ellenőrzési módszerrel. Adatváltozás esetén a Szolgáltató a bejelentést elfogadja telefonon történő bejelentéssel vagy minősített elektronikus aláírással hitelesített elektronikus kérelemmel is, de a megváltozott adatokat tartalmazó Tanúsítvány kiállításához szükséges az Aláíró személyes megjelenése, mert azonosítás-hitelesítését el kell végezni.

Az Ügyfélkapcsolati Iroda az időbélyegzés szolgáltatáshoz:

1. gondoskodik az Igénylő megfelelő azonosításáról,
2. regisztrálja az Ügyfelet,
3. az adatokat eljuttatja a technikai személyzethez, akik az időbélyegzés szolgáltatás adatbázisába rögzítik azokat,
4. szerződést köt,
5. az adatokat a szerződés fennállásáig megőrzi,
6. elszámolja és kiszámlázza a szolgáltatás ellenértékét,
7. kezeli az időbélyegzéssel kapcsolatos, az időbélyeg kérőktől, illetve az érintett felektől érkező bejelentéseket, kérdéseket, panaszokat.

2.1.6. Címtár feladatok és kötelezettségek

A Tanúsítványokkal kapcsolatos felfüggesztési, illetve visszavonási kérelmeket a Szolgáltató Ügyfélkapcsolati Irodája munkanapokon telefonon 8-16 óra között, személyesen az ügyfélfogadási időben (munkanapokon 9-13 óra között), illetve Ügyfélszolgálata (Help Desk-je) telefonon és elektronikus levélben folyamatosan (napi 24 órában) fogadja.

A Szolgáltató az Aláírás ellenőrző adatokat, továbbá a Visszavont Tanúsítványok Listáját (CRL) Címtárában közcélú Internet segítségével bárki számára hozzáférhető és folyamatosan elérhető módon közzéteszi.

A Címtár elérhetőségét a Szolgáltató folyamatosan[11], 99,9%-os rendelkezésre állással biztosítja úgy, hogy a Címtár szolgáltatás kiesése nem lépheti túl esetenként a 3 órás időtartamot.

A Címtár a kibocsátás szolgáltatás keretén belül:

1. közzé teszi az előfizetői tanúsítványokat[12];

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

a kibocsátott Tanúsítványokat a kibocsátást követően haladéktalanul, de legrosszabb esetben 1 órán belül közzé teszi a Címtárban;

2. biztosítja a 2. és a 3. pontokban szereplő információ folyamatos[13] elérhetőségét, még rendkívüli üzemeltetési helyzet esetén is;

annak érdekében, hogy a Címtár elérési útvonala bárki számára hozzáférhető legyen, Szolgáltató a 1.2 pontban, az Előfizetői Szerződésben és a **http://www.mavinformatika.hu/**ca/ weboldalon felsorolja azokat az Internet címeket, ahol a Hitelesítő Központonként vezetett nyilvántartások elérhetők. A Címtár elérési útvonala produktív Hitelesítő Központonként változhat.

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.

2. Biztosítja a legfrissebb Tanúsítvány visszavonási lista folyamatos[14] elérhetőségét, még rendkívüli üzemeltetési helyzet esetén is.

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

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. a leendő Előfizető az Ügyfélkapcsolati Irodánál személyesen megjelenő Igénylőt, aki a Tanúsítványt és az ezzel kapcsolatos műveleteket igényli, meghatalmazással ellátni, amennyiben az Igénylő nem maga az Előfizető,
2. az Igénylő a Tanúsítvány igénylése előtt megismerni és elfogadni a Szolgáltató általános szerződéses feltételeit és HSzSz-ét,

[12] Amennyiben az Aláíró hozzájárult ehhez.

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

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

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 eszközének és adatának, valamint a PIN kódjának védelmét,
9. az Aláíró Aláírás-létrehozó adatát aláírásra csak az Aláírás-létrehozó eszközzel használni;

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

10. az Előfizető, illetve az Aláíró 5 munkanapon belül jelezni Szolgáltatnál a regisztráció során felvett adataiban történő változásokat, különös tekintettel a Tanúsítványba foglalt adatokra,
11. az Előfizető az Aláíró figyelmét külön felhívni arra, ha az Előfizetői Szerződés a Tanúsítványfelhasználhatóságával kapcsolatban összeg, területi vagy egyéb korlátozásokat köthet ki,
12. az Aláíró az Aláírás-létrehozó adatát csak a vele közölt valamennyi korlátozásnak megfelelően használhatja,
13. az Aláíró tudomásul venni, hogy magánkulcsának védelme és az elektronikus aláírás készítése kizárólag a saját felelőssége, ezért ezzel - így különösen a magánkulcsának il-

letéktelen harmadik személyhez kerülésével - kapcsolatban a Szolgáltatót semmiféle felelősség nem terheli,

14. az Aláíró tájékoztatni az Érintett felet arról, hogy a HSzSz-ben meghatározott aláírás ellenőrzés lépéseinek elmulasztásából eredő következményekért az Érintett fél felel,
15. az Előfizető az ÁSzF módosításáról szóló értesítést követően 72 órán belül az aláírókat írásban tájékoztatni a változásokról;
16. amennyiben az Előfizető nem fogadja el az ÁSzF módosítását felmondási szándékát 5 naptári napon belül be kell jelentenie írásban az Ügyfélkapcsolati Irodánál, amely a felmondás beérkezését követő 10. naptári napig kezdeményezi a Tanúsítvány visszavonását,
17. az Aláíró azonnal, de legkésőbb a 10. pontban 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,
18. kompromittálódás esetén az Aláíró magánkulcsának használatát azonnal és véglegesen megszakítani,
19. az Előfizető az Előfizetői Szerződésben rögzített szolgáltatási díjakat a Szolgáltatónak megfizetni,
20. az Aláíró vagy az Előfizető a Tanúsítvánnyal ellátott elektronikus dokumentummal kapcsolatos jogvita megindulásáról köteles haladéktalanul tájékoztatni a Szolgáltatót,
21. az időbélyeget felhasználók kötelesek a kért időbélyeg vétele után meggyőződni arról, hogy:
    - ♦ az időbélyeget a Szolgáltató elektronikusan aláírta,
    - ♦ a Szolgáltató által történt aláírás az időbélyegzésre szolgáló kulccsal történt-e és a hozzátartozó Tanúsítvány érvényes-e;

a tanúsítvány érvényességét az időbélyeget felhasználók a 4.5.9 pont szerint meghatározott gyakorisággal közzétett CRL alapján ellenőrizhetik, amely a **http://www.mavinformatika.hu/ca/** web lapon keresztül érhető el.

Ezeken kívül:

1. az Aláíró jogosult arra, hogy a magánkulcsot birtokolja és a jogszabályokban meghatározott módon elektronikus aláíráshoz, 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 HSzSz-nek, valamint a hatályos jogszabályi rendelkezéseknek megfelelően használhatja; elektronikus aláírás csak Tanúsítvány érvényességi ideje alatt készíthető.

2.1.8. 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, 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,
8. Az időbélyeg aláíró kulcsa tanúsítványának az Érintett fél által történő ellenőrzésére vonatkozóan általában érvényesek a 2.2.8 pontban a tanúsítvány ellenőrzésre vonatkozó szabályok.

   Egy időbélyeggel ellátott állomány vétele után az Érintett félnek ellenőriznie kell a Szolgáltató általi aláírás megtörténtét, az Szolgáltató időbélyeg aláíró kulcsához tartozó Tanúsítvány érvényességét a CRL segítségével a 2.1.7 pontban leírt módon.

   Amennyiben az ellenőrzés a Tanúsítvány érvényességének lejárta után történik, akkor az elektronikus aláírásról szóló 2001. évi XXXV. törvény 9.§ (7. bek.) alapján a szolgáltatónál 10 évig, illetve az aláírt és/vagy időbélyegzett dokumentummal kapcsolatban felmerült jogvita lezárásáig megőrzött, a tanúsítványokkal kapcsolatos elektronikus információkat és ahhoz kapcsolódó személyes adatokat elő lehet keresni és a Tanúsítvány érvényességét ellenőrizni kell. A Tanúsítvány tartalmának megállapításához a Szolgáltatónak kell a megfelelő eszközt biztosítania.

2.2. A hitelesítés szolgáltató és felhasználó közösség tagjainak felelőssége

2.2.1. A MÁV INFORMATIKA Kft. felelőssége

Általános szabályok

- A MÁV INFORMATIKA Kft., mint Szolgáltató azzal, hogy aláír egy, a jelen HSzSz 1.4 pontja szerint meghatározott Tanúsítványt, illetve időbélyeget – az 1.3 pontban meghatározott felhasználó közösség és az érintett felek felé jelzi ezen HSzSz használatát –, csak azért vállalja a felelősséget, hogy a tanúsítvány előállítás, kibocsátás, közzététel, visszavonás, Visszavonási Lista közzététel és időbélyegzés tevékenységek a jelen HSzSz-ben előírtaknak teljes mértékben megfeleljenek, és a Szolgáltató megteszi a szükséges intézkedéseket, hogy a Szolgáltató maga és az előfizetők is a jelen HSzSz-nek megfelelően járjanak el.
- 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, illetve időbélyeg a jelen HSzSz-ben előírtaktól eltérő módon kerül felhasználásra. Így a Szolgáltató nem felelős az olyan károkért, mely abból adódott, hogy az Érintett fél a tanúsítványok vagy az időbélyegek ellenőrzése és felhasználása során nem a hatályos jogszabályok és a Szolgáltató szolgáltatói szabályzata szerint járt el, illetve nem tanúsította a tőle elvárható gondosságot.

A Szolgáltató felelősségére a következő részletes szabályok mérvadók:

- A Szolgáltató által okozott kárral kapcsolatos felelősségi és a kártérítési szabályt a 2.3 pont határozza meg.
- 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[15].
- A Szolgáltató kizárja felelősségét, ha az aláírás vagy az időbélyeg ellenőrzés lépései a jelen HSzSz alapján bármi okból – beleértve Szolgáltatónál keletkező üzemeltetési problémát is – nem hajthatóak végre az aláírás vagy az időbélyeg ellenőrzésének időpontjában, és az elektronikus aláírás vagy az időbélyeg, az ellenőrző személy által ennek ellenére elfogadásra kerül.
- Szolgáltató HSzSz-e vagy az Előfizetői Szerződés megszegéséből származó károk esetén a vele szerződéses jogviszonyban álló Előfizetővel szemben a Polgári Törvénykönyv szerződésszegésért való felelősség szabályai szerint felelős.
- 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 pont rendelkezik.

2.2.2. A Hitelesítő Központok felelőssége

A Hitelesítő Központok felelősségének belső megosztása nem érinti a szolgáltató társaság egységes jogi felelősségét.

Az 1. szintű „Root CA” felelős a közvetlenül alá rendelt hitelesítő központok és szervezetek hitelesítésért.

Nem felelős az alá rendelt Hitelesítő Központok működéséért.

A 2. szintű „Produktív CA” felelős:

- az általa kibocsátott tanúsítványok hitelességéért.
- az általa létrehozott alárendelt hitelesítő központok hitelesítésért,

[15] A Szolgáltató általánosan felelős a Hitelesítő Központok, a Regisztrációs és az Ügyfélkapcsolati Irodák, valamint a Címtár kötelezettségeiért, tevékenységeiért.

- 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. A Szolgáltató felelőssége az időbélyegzés szolgáltatás vonatkozásában

A Szolgáltató felelős azért, hogy:

- az időbélyegző válasz, az időbélyegzéssel összefüggésben hozzáadottaktól eltekintve, ugyanazokat az adatokat tartalmazza, amelyeket a kérelem tartalmazott,
- a kibocsátott időbélyeg ne tartalmazzon hibás adatot,
- az időbélyeg aláíró kulcs csak az időbélyegzés keretén belül kerüljön felhasználásra,
- az időbélyeg 1 másodpercen belüli pontossággal kerüljön kiadásra,
- az időbélyegzési rendszer belső órája 0,1 másodperc pontossággal szinkronizálásra kerüljön az UTC időalaphoz.
- az időbélyegzés szolgáltatás rendelkezésre állása nem legyen rosszabb, mint 99,5%,
- az időbélyeg aláíró kulcs 2/2002. (IV. 26.) MeHVM irányelv 212. pont szerint tanúsított kriptográfiai modulban kerüljön előállításra és tárolásra, az a teljes életciklusa folyamán nem hagyhatja el a modult,
- olyan fizikai és személyi környezetet biztosítson, amely fokozott biztonsági szinten védi az aláíró kulcs bizalmasságát, hitelességét és sértetlenségét,
- az időbélyegzéssel kapcsolatos minden esemény biztonságos módon rögzítésre, naplózásra és archiválásra kerüljön.

2.2.4. Hitelesítési Politika és Szabályozási Csoport felelőssége

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

2.2.5. A Regisztrációs Iroda felelőssége

A Regisztrációs Iroda felelős:

- a regisztrációs adatok 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.

2.2.6. Az Ügyfélkapcsolati Iroda felelőssége

Az Ügyfélkapcsolati Iroda felelős:

- az előfizetők személyazonosságának és szervezeti identitásának megállapításáért és a bemutatott dokumentumok alapján történő ellenőrzéséért,
- a felvett regisztrációs adatok ellenőrzéséért,
- a regisztrációs adatoknak a Regisztrációs Irodához történő bizalmas, hiteles és sértetlen eljuttatásáért,
- a tanúsítvány visszavonási igény bejelentője személyazonosságának és szervezeti identitásának megállapításáért és a bemutatott dokumentumok alapján történő ellenőrzéséért,
- az előfizetői pénzkezeléséért.

2.2.7. Az Aláíró és az Előfizető felelőssége

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

Az Előfizetőnek kártérítési felelőssége áll fenn a Szolgáltatóval szemben azokért a veszteségekért és károkért, melyeket a regisztráció során megadott helytelen adataival, vagy az azokban bekövetkezett változások be nem jelentésével, vagy egyéb kötelezettségeinek be nem tar-

tásával számára okoz. Az Előfizető felelős azért, ha magánkulcsát nem a HSzSz-ben, az ÁSzF-ben és a vonatkozó jogszabályokban meghatározott módon és célra használta.

Az Előfizető és az Aláíró felelős az Aláírás-létrehozó eszköz biztonságos megőrzéséért, az Aláírás-létrehozó eszköz adat és a PIN kód illetéktelenek tudomására jutásának megakadályozásáért.

Az időbélyeget kérő fél felelős az időbélyeg aláírás helyességének és az időbélyeg aláíró kulcs Tanúsítványa érvényességének az időbélyegzett állomány vételekor elvégzendő, a 2.1.7 pont szerinti ellenőrzésért.

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.

2.2.8. 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 2.1.8 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 jelen 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 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 HSzSz-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 az ÁSzF-ben, illetve az Előfizetői Szerződésben megjelölt összeghatárig köteles kártérítésre.

A Szolgáltatásokkal 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 és időbélyegeket bocsát ki, semmilyen körülmények között nem tekinthető az előfizetők vagy az érintett felek ügynöké-

nek, 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 4.6 és 4.7 alfejezeteket.)

A Szolgáltató Szervezeti és Működési Szabályzatában kerültek meghatározásra azok az adminisztrációs folyamatok, amelyek a Biztonságos aláírás létrehozó eszköz, a Tanúsítvány és az időbélyeg kibocsátást támogatják.

Ilyenek:

- az igénylők adatainak nyilvántartása, tárolása, archiválása,
- az előfizetők, aláírók tanúsítványainak, a Visszavonási listák tárolása, archiválása,
- számlázás, számlázási adatok nyilvántartása, archiválása,
- a Szolgáltató által üzemeltetett Trust&Sign Rendszer elemeinek nyilvántartása,
- a hitelesítési tevékenységek, valamint biztonsági audit eljárások,
- minőségbiztosítási eljárások.

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[16]
- 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 aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.
- 15/2001. (VIII. 27.) MeHVM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról.
- 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.
- 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,

[16] A 2001. évi XXXV. törvényt kiegészítő, felsorolt alacsonyabb szintű jogszabályok a 2002 május 31.-i állapotot tükrözik.

- 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 és 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 HSzSz 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

Jelen HSzSz időbeli hatálya az 1.3.6.1 pontnak megfelelően a Hírközlési Felügyelet nyilvántartásba vételének keltétől a szolgáltatási tevékenység megszűntéig tart. A HSzSz személyi és tárgyi hatályát az 1.3.6.1 pont tartalmazza.

Jelen HSzSz 2. fejezete érvényben marad a HSzSz 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 HSzSz és az ÁSzF a közösség résztvevőinek valamennyi kötelezettségét, felelősségét és jogát tartalmazza. A HSzSz 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 HSzSz csak írott és hitelesített formában módosítható, a Hírközlési Felügyelet által vezetett tanúsítványtípus nyilvántartásban való átvezetés mellett.

A jelen HSzSz a Szolgáltató működésének befejezésével tekintendő megszűntnek.

2.4.2.4. Értesítések

Az előfizetők, az érintett felek vagy bármely harmadik fél az Ügyfélkapcsolati Irodát naponta 9-13 óráig megkeresheti személyesen telefonon, írásban, e-mail-ben vagy faxon. Naponta 24 órás szolgálattal áll rendelkezésre telefonos vagy e-mail megkeresés esetén a Szolgáltató Ügyfélszolgálata (Help Desk-je). A telefonszámokat és az e-mail címeket az 1.5.1 pont tartalmazza. 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 Ügyfélkapcsolati Irodán 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.

A panaszt az Előfizetőt nyilvántartó Szolgáltató Ügyfélkapcsolati Irodán vagy az Ügyfélszolgálatnál (Help Desk-nél) lehet írásban vagy szóban előterjeszteni az 1.5.1. pontban megadott elérhetőségekkel és időpontokban. A panasz kézhezvételéről a Szolgáltató az érkeztetést követően 24 órán belül értesíti a bejelentőt, a megjelölt címen, az ügy kivizsgálásához szükséges idő megjelölésével. A jelzett időn belül, – mely nem lehet több, mint 10 munkanap –, a Szolgáltató írásban válaszol a bejelentőnek. Ha a választ bejelentő nem fogadja el, egyeztetést kell kezdeményeznie Szolgáltatóval.

Ha a Szolgáltató ezt megtagadja, vagy ha a felek közötti egyeztetés annak megkezdésétől számított 30 munkanapon belül nem vezetne eredményre, akkor a bejelentő jogi útra terelheti

az ügyet. Ez esetben felek kölcsönösen alávetik 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 HSzSz-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 HSzSz-ben szereplő kifejezéseket és jogintézményeket a magyar nyelv szabályai 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 keresztül 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

Szolgáltató a kibocsátott tanúsítványokért éves fenntartási díjat számol fel az Előfizető felé, amely tartalmazza a Tanúsítvány kibocsátásának, címtárban történő közzétételének az érvényesség időtartamára, valamint lejárat utáni archiválásának a költségét.

A 3.2 pont szerinti Tanúsítvány frissítés esetén a Szolgáltató díjat számol fel.

2.5.2. Tanúsítvány hozzáférés

A Szolgáltató a 2.6.4 pontban közzétett tanúsítványok eléréséért nem számol fel díjat az érintett felek irányában.

2.5.3. Visszavonási lista hozzáférés

A Szolgáltató a közzétett visszavonási lista eléréséért nem számol fel díjat az érintett felek irányában.

2.5.4. Időbélyegzés

A Szolgáltató az időbélyegek kibocsátásáért díjat számol fel. A Szolgáltató az időbélyegek kibocsátását a Trust&Sign® Időpecsételés Szolgáltatás márkanéven forgalmazza. A díj mértéke a 2.5 pontban megadott elérhetőségen keresztül tekinthető meg.

2.5.5. Egyéb szolgáltatásokra vonatkozó díjak

Szolgáltató a kibocsátott tanúsítványok visszavonásáért és újraérvényesítéséért eljárási díjat számol fel az Előfizető felé, mely tartalmazza a Tanúsítvány megváltozott állapotának a címtárban visszavonási lista formájában történő közzétételének költségét. Újraérvényesítésért csak abban az esetben számít fel a Szolgáltató díjat, ha a felfüggesztést az Aláíró vagy az Előfizető kérte.

2.5.6. Visszatérítési elvek

Az Előfizető a számára kibocsátott Tanúsítvány éves fenntartási díjának visszatérítésére a következő esetekben jogosult:

- a kibocsátott Tanúsítvány valamely adata a Szolgáltató hibájából fakadóan nem megfelelő,
- a kibocsátott Tanúsítvány, magánkulcs és aktivizáló adat nem összetartozó,
- a kibocsátott Aláírás-létrehozó eszközön szereplő adatok a Szolgáltató hibájából fakadóan nem megfelelők,[17]
- a kibocsátott Aláírás-létrehozó eszköz, az aktivizáló kód és a kulcsok nem összetartozók,
- a Szolgáltató bizonyítottan nem tartja be valamely kötelezettségét Előfizető Tanúsítványának kezelésekor.

A díj visszatérítésére az Előfizetőnek a Tanúsítvány kibocsátását, illetve megújítását követő 30 naptári napon belül a regisztrációt végző regisztráló szervezetnél kérvényt[18] kell beadnia szolgáltató részére. A kérvény pozitív elbírálása esetén a Szolgáltató a Tanúsítványt díjmentesen visszavonja és a fenntartási díjat az Előfizető számára a megjelölt bankszámlaszámra 20 naptári napon belül visszautalja.

A Tanúsítvány kibocsátását, illetve megújítását követő 30 naptári napon túl az Előfizető kizárólag csak a Szolgáltató bizonyított szerződés- vagy kötelezettségszegése esetén jogosult díjvisszafizetésre.

A Szolgáltató egyéb tevékenységeiért számlázott díjak esetében díjvisszafizetésre nem köteles.

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:

[17] Pl. a kártya fizikai megszemélyesítése nem megfelelő.

[18] Erre vonatkozóan a Szolgáltatónak formanyomtatvánnyal rendelkezik.

- 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 2.1.7 alfejezetben meghatározottaknak megfelelően,
  - a Tanúsítvány ellenőrzésének mikéntjére vonatkozó információ, beleértve a tanúsítvány visszavonási állapot ellenőrzésére vonatkozó követelményeket, oly módon, hogy az Érintett fél "ésszerű módon hagyatkozhasson" a Tanúsítványra (lásd 2.1.8),
  - a felelősség vállalásra 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 4.7) megőrzik,
  - az az időtartam, amíg a Szolgáltató eseménynaplóját (lásd 4.6.3) 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 a „**http://www.mavinformatika.hu**/ca/” 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 a HSzSz-ében 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.

A Szolgáltató információ közzétételi kötelezettségét az alábbiak szerint teljesíti:

- a Szolgáltató http://www.mavinformatika.hu/ca/ honlapján keresztül teszi közzé a szolgáltatás beindítását az 1. szintű Hitelesítő Központ Tanúsítványának aláírásával, a szolgáltatás beszüntetését, új tanúsítványtípus, osztály vagy fajta bevezetését, valamint magánkulcsának kompromittálódását, amennyiben ilyen esemény bekövetkezik.

A Szolgáltató az általa működtetett hitelesítő egységek Tanúsítványát a következő módszerekkel teheti közzé:

- Az 1. szintű Hitelesítő Központ ("Root"; önhitelesített) Tanúsítványát a http://www.mavinformatika.hu/CA/ web lapon keresztül teszi közzé. A Root tanúsítványok esetében ez az egyetlen módszer tekinthető hivatalos formának.
- Minden nyilvános Hitelesítő Központ és az időbélyegző központ Tanúsítványát közzé teszi Internetes honlapján keresztül.
- Az egyes Hitelesítő Központok Tanúsítványa beépítésre kerülhet különböző alkalmazásokba.
- Az Előfizető részére az előfizetői tanúsítvánnyal együtt átadja (lásd 4.2 pont!).

♦ A Szolgáltató a Címtárban tárolja és az internetes honlapon teszi elérhetővé a kibocsátott tanúsítványokat, köztük az Root, a produktív Hitelesítő Központok tanúsítványainak és az időbélyeg aláíró kulcs Tanúsítványát, a tanúsítvány visszavonási listákat.

♦ A Szolgáltató saját web oldalain keresztül elérhetővé teszi a HSzSz-t, az ÁSzF-et, az egyéb nyilvános szabályzatokat és vonatkozó alkalmazásokat, valamint az Ügyfélszolgálati Irodák listáját, elérhetőségét az 1.2 pontban megadott elérhetőséggel.

♦ Szolgáltatónak csak saját elektronikus aláírásával ellátott dokumentumai tekinthetők eredetinek. A dokumentumok nyomtatott változatai semmilyen formában sem tekinthetők hivatalos példánynak vagy hiteles másolatnak.

Szolgáltató az általa kibocsátott előfizetői tanúsítványokat a következő módszerek egyikével juttatja el Ügyfeleinek:

♦ A kérelmező Aláíró részére elküldi védett kommunikációs protokollt alkalmazva.

♦ A kérelmező Aláíró részére átadja Biztonságos aláírás-létrehozó eszközön.

♦ Az érintett felek részére közzéteszi az internetes honlapján, amennyiben ehhez az Aláíró és az előfizető hozzájárult (a hozzájárulás formája a tanúsítványigénylő űrlapon ennek írásos jelölése).

A Szolgáltató az általa működtetett Hitelesítő Központok Tanúsítványával kapcsolatos állapot információkat a következő módszerekkel teszi közzé:

♦ Az 1. szintű (Root) Hitelesítő Központ Tanúsítványának állapotváltozását a http://www.mavinformatika.hu/ca/ vagy a http://crl.trust-sign.hu web lapon keresztül te-

szi közzé. A root tanúsítványok esetében ez az egyetlen módszer tekinthető hivatalos formának.

- A 2. szintű (Produktív) Hitelesítő Központok tanúsítványainak és az időbélyeg aláíró kulcs Tanúsítványának állapotváltozását a Címtárában hozza nyilvánosságra.

A Szolgáltató az általa kibocsátott előfizetői tanúsítványokkal kapcsolatos állapot információkat a fent web lapokon hozza nyilvánosságra.

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 4.5.9 pontnak megfelelő gyakorisággal tesz közzé.

A Szolgáltató a HSzSz-ben és az ÁSzF-ben tervezett változásokról a hatályba lépést megelőzően 30 nappal tájékoztatja a Hírközlési Felügyeletet, s a változásokkal egységes szerkezetbe foglalva közzéteszi, egyéb nyilvános szabályzatait pedig a hatályba lépést megelőző 30 nappal hozza nyilvánosságra.

A Szolgáltató az egyes tanúsítványok nyilvánosságra hozatala kapcsán a következő gyakorlatot követi:

- Az általa működtetett root hitelesítő egységek Tanúsítványát a kibocsátást követő 10 munkanapon belül teszi közzé.
- Az általa működtetett 2. szintű Hitelesítő Központok tanúsítványai és az időbélyeg aláíró kulcs Tanúsítványa a Címtárában 24 órán belül, Internetes honlapján 5 munkanapon belül megjelennek.
- A Szolgáltató az előfizetői tanúsítványokat a kibocsátást követően, a regisztráló eljárás részeként átadja az Előfizető részére.
- A Szolgáltató az előfizetői tanúsítványokat a honlapján keresztül az előállítást követően 24 órán belül teszi közzé.

2.6.3. Elérési szabályok

A Szolgáltató a nyilvánosságnak bocsát ki Tanúsítványt és időbélyeget, ezért a tanúsítványok és az időbélyegek, valamint azok 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, 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 adatait.

A Címtár elérhetőségét a Szolgáltató folyamatosan (az év minden napján, 0-24h), 99,9%-os rendelkezésre állással biztosítja, a karbantartáshoz szükséges idők kivételével úgy, hogy a Címtár szolgáltatás kiesése nem lépheti túl esetenként a 3 órás időtartamot.

2.7. A megfelelőség vizsgálata

A Szolgáltató olyan biztonságos 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. Konkrét ismertetésük a HSzSz 6.1.7 és 6.2.1 pontjaiban szerepel.

A Szolgáltató az „Aláírás-létrehozó eszközön az Aláírás-létrehozó adat elhelyezése” szolgáltatásához olyan biztonságos aláírás létrehozó eszközt használ fel, mely szerepel a Hírközlési Felügyelet „tanúsított elektronikus aláírási termékek” listáján. Konkrét ismertetésük a HSzSz 6.1.7 és 6.2.1 pontjaiban szerepel.

A Szolgáltató az időbélyegzés szolgáltatásához olyan biztonságos aláírás létrehozó eszközt használ fel, mely szerepel a Hírközlési Felügyelet „tanúsított elektronikus aláírási termékek” listáján. Konkrét ismertetésük a HSzSz 6.1.7 és 6.2.1 pontjaiban szerepel.

A Szolgáltató a hitelesítő és időbélyegzési tevékenységét és a hitelesítés és időbélyegzés szolgáltatást támogató informatikai rendszer, valamint annak személyi és fizikai környezetének biztonságát auditáltatja:

1. a saját szervezetén belüli, a Szervezeti és Működési Szabályzatban megjelölt, nem a Szolgáltató alá rendelt, belső auditor szervezettel,
2. független külső auditor céggel.

A Szolgáltató a szolgáltatási rendszerének következő elemeit tanúsíttatja:

- az aláírás-létrehozó eszközét, melyet magánkulcsainak tárolására használ.
- a biztonságos aláírás-létrehozó eszközöket, melyeket az előfizetők számára biztosít.

A Szolgáltató a szolgáltatási rendszerének következő elemeit auditáltatja:

- Az előfizetői és szolgáltatói minősített tanúsítványok kezeléshez és az időbélyegzéshez felhasznált elektronikus aláírási termékeit.
- Az előfizetői és szolgáltatói minősített tanúsítványok kezeléshez és az időbélyegzéshez használt rendszereit és módszereit.

A tanúsításhoz a Szolgáltató külső szervezetet vesz igénybe (lásd 2.7.2 pont!). Szolgáltató e külső tanúsításokon túl saját belső ellenőrzési rendszerrel is rendelkezik, mely rendszeresen

vizsgálja a korábbi tanúsításoknak való megfelelőséget, s eltérés esetén megteszi a szükséges lépéseket.

2.7.1. Vizsgálatok gyakorisága

A biztonságos aláírás létrehozó és az aláíró eszközök tanúsítására egyszer kerül sor, a használatba vételt megelőzően.

A minősített tanúsítványok kezeléshez használt rendszerek és módszerek tanúsítására hatósági minősítési eljárás keretében kerül sor.

A szolgáltatások megindítása után a Hírközlési Felügyelet a jogszabályoknak megfelelően legalább évente átfogó helyszíni ellenőrzést végez vagy végeztet.[19]

A Szolgáltató által megrendelt külső, illetve a saját ellenőrző szervezete által végzett belső vizsgálatokat Szolgáltató a Szervezeti és Működési Szabályzatban, illetve a Biztonsági Szabályzatban megjelölt rendszerességgel, minimum évente egyszer megismételteti, azt a törvényi feltételek vagy szabályzataiban bekövetkezett jelentősebb változások esetén, döntése alapján, soron kívül elvégezteti.

2.7.2. Az átvizsgáló szervezet megnevezése/jellemzői

A belső hitelesítési tevékenységre és az informatikai biztonságra vonatkozó auditot a Szolgáltató informatikai biztonsági menedzsere, a külső auditot a Szolgáltató olyan, széles körben ismert auditor céggel végezteti el, amely szakértelmét bizonyítani tudja a nyilvános kulcsú infrastruktúra, és informatikai biztonság, valamint az ezen területekre vonatkozó technikai, technológiai, jogi, szabályzati ismeretek és auditálási módszertanok vonatkozásában.

Az auditot a hitelesítés szolgáltatás minősítési kérelmének beadása előtt az EDIPORT Kft. végezte el. Az auditálás folyamatát és eredményét a Hírközlési Felügyelet szakértői listájában szereplő Erdősi Péter Máté ellenőrizte.

Ezután a rendszeres auditálások a HSzSz 6.5.2 pontja szerinti rendben történnek.

[19] 2001. évi XXXV. törvény 8, 18, 20. § alapján

2.7.3. Az átvizsgáló szervezet és a vizsgált fél kapcsolata

A belső auditot a Szolgáltató hitelesítés és időbélyegzés szolgáltatást végző szervezeti egységétől független informatikai biztonsági menedzser, a külső auditot a Szolgáltatótól és a nyilvános kulcsú infrastruktúra, illetve informatikai biztonsági termék és szállítótól független külső auditor cég végzi el**.** A Szolgáltató által kezdeményezett auditok vizsgálati jelentését az auditor a Szolgáltató vezetőjének és a Hitelesítési Politika és Szabályozási Csoportnak nyújtja be.

Az auditokat a Szolgáltató belső ellenőre és minőségbiztosítási vezetője ellenjegyzi. A Szolgáltató outsourcing üzletág igazgatója és PKI Üzleti Egység vezetője tőlük írásos javaslatot kap.

2.7.4. A vizsgálatok kiterjedése

A belső vizsgálatok a Szolgáltató tanúsítványtípusainak, a mindenkori hatályos törvényi előírásoknak, valamint a Szolgáltató saját szabályzatainak, első sorban a Hitelesítési Politikáknak, az Időbélyegzés Szolgáltatási Politikának, a Hitelesítés Szolgáltatási Szabályzatának, a Trust&Sign Biztonságpolitikának és a Trust@Sign Biztonsági Szabályzatnak való megfelelést fedi le.

A minősített tanúsítványok kezelése és az időbélyegzéshez használt rendszerek és módszerek tanúsítása a 2001. évi XXXV. törvény 3. számú mellékletének és a 16/2001. (IX. 1.) MeHVM rendelet előírásainak, valamint Szolgáltató saját HP-inek, az ISzP-nek és egyéb szabályzatainak való megfelelőség vizsgálatára irányul.

A Biztonságos aláírás létrehozó és aláíró eszközök tanúsítása a 2001. évi XXXV. törvény 1. számú mellékletének való megfelelőség vizsgálatára irányul.

2.7.5. Hiányosságok kezelése

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

A Szolgáltató által kezdeményezett audit jelentésben megállapított hiányosságok következménye két szintű lehet:

1. A hiányosságok nem sértik alapvetően a Szolgáltató tevékenységébe vetett bizalmat, vagy az informatikai biztonságot. A Szolgáltató változatlan formában folytatja tevékenységét, de köteles a hiányosságokat 30 napon belül megszüntetni.
   A hiányosságok megszüntetésére vonatkozó konkrét intézkedéseket a Hitelesítési Politika és Szabályozási Csoport dolgozza ki és ellenőrzi a végrehajtásukat.
   Az intézkedéseket a Szolgáltató első számú vezetője hagyja jóvá.

   Amennyiben a korrekciós intézkedések 30 napon belül nem kerülnek végrehajtásra, akkor a Szolgáltatónak a hiányosságok által érintett funkcióit, tevékenységét fel kell függesztenie az intézkedések ellenőrzésének befejezéséig. Amennyiben ez a létrehozandó aláírás létrehozó adatok, eszközök biztonságát vagy a tanúsítványok, visszavonási listák hitelességét veszélyezteti, akkor ezen tevékenységet és a tanúsítványokat fel kell függeszteni.
2. Amennyiben a hiányosságok alapvetően érintik a Szolgáltató tevékenységét, vagy az informatikai biztonságot, a Szolgáltatónak fel kell függesztenie a hiányosságok által érintett tevékenységeit a hiányosságok megszüntetéséig. Amennyiben ez a létrehozandó aláírás létrehozó adatok, eszközök biztonságát vagy a tanúsítványok, visszavonási listák hitelességét veszélyezteti, akkor ezen tevékenységet és a kibocsátott tanúsítványokat fel kell függeszteni. A hiányosságokról, azok kiküszöbölésére vonatkozó intézkedésekről és azok határidejéről a Szolgáltatónak a Hírközlési Felügyeletet tájékoztatnia kell. A hiányosságok megszüntetésére vonatkozó konkrét intézkedéseket a Hitelesítési Politika és Szabályozási Csoport dolgozza ki és ellenőrzi a végrehajtásukat. Az intézkedéseket a Szolgáltató első számú vezetője hagyja jóvá.
3. Amennyiben a hiányosságok a Szolgáltatóba vetett bizalmat alapvetően megingatják, a teljes tevékenységét fel kell függeszteni és a kibocsátott tanúsítványokat vissza kell vonni. A tevékenység felfüggesztésének okáról, a szolgáltatás visszaállítása érdekében megvalósított vagy megvalósítandó intézkedésekről és azok határidejéről a Szolgáltatónak a Hírközlési Felügyeletet tájékoztatnia kell.

2.7.6. Eredmény kommunikációja

A Hitelesítési Politika és Szabályozási Csoport javaslatot tesz arra, hogy az audit jelentés mely részei tekintendők publikusak.

A javaslatot a Szolgáltató vezetője hagyja jóvá. A teljes jelentés belső használatra szolgáló anyag. Azt a Szervezeti és Működési Szabályzatban meghatározott szervezeti egységek vezetői kapják meg. A publikus részt a Szolgáltató a **http://www.mavinformatika.hu/**ca/ web oldalon keresztül teszi közzé.

A Szolgáltató nem köteles a feltárt konkrét hiányosságokat nyilvánosságra hozni, és ebben az esetben azok nem adhatnak alapot a Szolgáltató kötelezettségszegésének bizonyítására. Szolgáltató nem tartozik kártérítési felelősséggel az általa elvégeztetett vizsgálatok alapján feltárt hibák után.

2.8. Bizalmasság – Adatkezelési szabályzat

2.8.1. Bizalmas információk

A Szolgáltató gondoskodik 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 4.6 és 4.7),
- 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 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[20] hozzájárulnak, vagy ha bíróság, illetve egyéb jogi követelmény ezt előírja,
- védi a regisztrációs adatok bizalmasságát (és sértetlenségét) az előfizetővel/alannyal folytatott, illetve a hitelesítő szervezet – regisztráló szervezet – címtár rendszerkomponensek közötti adatcsere során is.

A legmagasabb érzékenységi szintet bizalmasság szempontjából az aláírók és a hitelesítés szolgáltatók aláírás létrehozó adatai képezik, ezen belül a legérzékenyebb a szolgáltatói Aláírás létrehozó adat, mert kompromittálódása a Szolgáltató tevékenységének azonnali felfüggesztésével jár. Ezért ezeket az adatokat, illetve az ezeket hordozó eszközöket fokozott biztonsággal kell tárolni és használni. Az Aláírás létrehozó adat biztonságáért a teljes felelősséget az adat tulajdonosa viseli.

A Szolgáltató tevékenysége során a következő bizalmas adatköröket kezeli:

1. a Szolgáltató üzleti titkai,
2. más Társaságok által a Szolgáltatónak átadott üzleti titkok,
3. az előfizetők, az aláírók és a saját munkatársainak személyes adatai,
4. magánkulcsok és aktivizáló kódok,
5. tanúsítványigénylések és előfizetői szerződések,
6. tranzakciós és napló adatok,
7. nem nyilvános szabályzatok,
8. minden olyan adat, amelynek nyilvánosságra kerülése a szolgáltatások biztonságát előnytelenül befolyásolná.

Az 1. és 2. pontokban meghatározott üzleti titkok kezelésére az 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról és a Szolgáltató Titokvédelmi Szabályzata mérvadó. Így például egyik szerződő fél sem jogosult az Előfizetői Szerződés

[20] vagy nevükben az Előfizető

teljesítése kapcsán tudomására jutott bármely adatot, tényt, információt, tervet vagy dokumentumot a másik fél előzetes írásbeli hozzájárulása nélkül harmadik személynek átadni.

A felek az üzleti titok megsértésével okozott kárért a polgári jog általános szabályai szerint felelnek.

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. törvény módosításáról szóló törvény.

A fentiek értelmében a Szolgáltató az előfizetők és az aláírók személyes adatait csak a közöttük fennálló Előfizetői Szerződéssel összhangban levő célokra használhatja fel, harmadik félnek azokat az előfizetők és az aláírók írásos hozzájárulása nélkül nem adhatja át, kivéve a 2.8.4 pontban meghatározott eseteket. A Szolgáltató a birtokába került személyes adatokat az adott adat rögzítéséhez kapcsolódó Tanúsítvány lejártát, illetve a tanúsítvánnyal összefüggésbe hozható jogi eljárás lezárását követő 10 évig (2001. évi XXXV. törvény 9.§(7.) bek.) őrzi meg.

Az Előfizető és az Aláíró a Tanúsítvány igénylésével a hozzájárul ahhoz, hogy a Szolgáltató személyes adatait (a Titokvédelmi és a Biztonsági Szabályzatainak megfelelő módon) tárolja és kezelje. A hozzájárulás egyaránt vonatkozik az adatoknak az Aláíróval és Előfizetővel való megosztására (ha a két fél különbözik), s nyilvántartásba vett információk harmadik félhez történő továbbítására, a szolgáltató szolgáltatásainak leállítása esetén[21]. A tanúsítványigénylő űrlapon az Előfizetőnek és az Aláírónak jeleznie kell a Tanúsítvány nyilvánosságra hozatalához történő egyhangú hozzájárulását. Szolgáltató az előfizetői adatokat kizárólag csak a hitelesítési-szolgáltatással összefüggésben használja fel.

A Szolgáltató által kezelt adatok egy része a Tanúsítványba foglalva, valamint a Szolgáltató címtárán keresztül nyilvánosságra kerül a nyilvános kulcs tulajdonosának azonosítása céljából, másik részét a Szolgáltató védett módon tárolja az Előfizető és az Aláíró azonosságának igazolása és egyéb adatszolgáltatási kötelezettségei céljából.

[21] 2001. évi XXXV. tv. az elektronikus aláírásról 16. § (2) bek.

2.8.2. Nem bizalmas információk

A Szolgáltató nem bizalmas információként kezeli mindazon adatokat, melyet a Tanúsítványba belefoglal[22]. Az Előfizető és az Aláíró tudomására kell hozni szerződéskötéskor, hogy mely személyes adatai fognak a Címtárban hozzáférhető tanúsítványokban szerepelni és a regisztrációs lapon ezeket külön jelölni kell.

Nem bizalmas információk, adatok még azok a Szolgáltatóhoz kapcsolódó adatok is, amelyeket a Szolgáltató vezetője publikusnak minősít, illetve amelyekről a hatályos jogszabályok így rendelkeznek.

2.8.3. Tanúsítvány visszavonási és felfüggesztési okok felfedése

A Szolgáltatónak az általa kibocsátott tanúsítványok visszavonását és felfüggesztését tanúsítvány visszavonási listákban (CRL[23]) teszi közzé, a 7.2 pontban meghatározott tartalommal, jellemzőkkel, illetve az ezekben általa támogatott keresési lehetőségekkel.

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

2.8.4. Feltárás törvényi meghatalmazással rendelkezők részére

A Szolgáltató az elektronikus aláírás vagy az időbélyeg felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből – az érintett személyazonosságát igazoló adatok tekintetében - a 2001. évi XXXV. törvény 11.§ (3) bekezdése alapján adatokat továbbít a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak.
Az adatátadás tényét rögzíteni kell, az adatátadásról a Szolgáltató az Aláírót nem tájékoztathatja.

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

[23] CRL: Certification Revocation List

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. Feltárás tulajdonos kérésére

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

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.

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

A Tanúsítványban szereplő megkülönböztető név használatára a megnevezett Tulajdonos 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 Szolgáltató az elektronikus aláíráshoz szükséges Tanúsítvány igénylésekor végrehajtandó kezdeti regisztrálás során:

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

Ha egy Igénylő csak időbélyegzés szolgáltatást igényel, a kezdeti regisztráció egyszerűsített eljárással történik a 3.1.10 pont szerint.

3.1.1. Nevek típusa

A tanúsítványokban szereplő név (Kibocsátó, illetve Aláíró név) megadás az ITU-T X.500 „Information Technology - Open Systems Interconnection - The directory: Overview of concepts, models and services" ajánlása egyedi név formátum (Distinguished Name form) előírásainak felel meg.

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 Kibocsátó névmegadása a következő módon épül fel, a MÁV Informatika Kft. PKI Üzleti Egységére vonatkozó tanúsítvány névmegadási példájával illusztrálva[24]:

Mezőnév	Mező tartalma
Country (C)[25]:	HU
Locality (L):	Helységnév, pl. Budapest
State:	Nem kitöltött

[24] 2001. évi XXXV. tv. az elektronikus aláírásról 2. számú melléklet b) pont.

[25] Az RFC 3039 3.1.1 fejezetének és az ETSI TS 101 862 4.1 fejezetének megfelelően. Az ISO 3166 szabvány szerinti két karakteres országkódokat kell alkalmazni.

Mezőnév	Mező tartalma
Organization (O):	A Szolgáltató szervezet neve, pl. MÁV INFORMATIKA Kft.
Organizational unit (OU):	A Szolgáltató szervezet egység neve, pl. PKI Services BU
Common Name (CN):	Minősített Szolgáltató kibocsátást végző hitelesítő központjának neve, pl. Trust&Sign QCA V1.0
STREET:	Cím, pl. Krisztina krt. 37/A.
PostalCode:	Irányítószám, pl. 1012
Email:	e-mail cím, pl. ica@mavinformatika.hu

A tulajdonosazonosító a következő módon épül fel szervezeti személy számára kibocsátott Tanúsítvány példájával illusztrálva:

Mezőnév	**Mező tartalma**	**Kitöltési szabály**
Country (C):	Az Előfizető szervezet székhelye vagy telephelye szerinti ország, pl. *HU*	Tanúsítványigénylő űrlapnak megfelelően.
Locality (L):	Az Előfizető szervezet székhelye vagy telephelye szerinti város, pl. *Budapest*	Tanúsítványigénylő űrlapnak megfelelően.
State:	Nem kitöltött	Üresen kell hagyni.
Organization (O):	Az Előfizető szervezet hivatalos neve, pl. *MÁV INFORMATIKA Kft.*	Szervezet alapító okirata szerint. Gazdasági társaság esetében a cégbe-jegyzésben szereplő rövid név és a szervezet típusa.
Organizational unit (OU)[26]:	Az Aláíró szervezeti egységének neve, pl. *Üzemeltetési Üzleti Egység*	Tanúsítványigénylő űrlapnak megfelelően.
Common Name (CN):	Alany családi és keresztneve, pl. Kiss József	Személyazonosító okmányban szereplő formátum. Egyediséget biztosító sorszám, ha szükséges.
STREET:	Az Aláíró teljes címének utca, házszám része, pl. *Bocskai úi 46.*	Tanúsítványigénylő űrlapnak megfelelően.
PostalCode:	Az Aláíró teljes címének irányítószám része,	Tanúsítványigénylő űrlapnak megfelelően.

[26] Az Organizational unit mezőt igen gyakran többször is használják (szervezeti egységen belüli szervezeti egység). Ha ilyenre kerül sor, akkor azt jelezni kell.

Mezőnév	Mező tartalma	Kitöltési szabály
	pl. *1113*	
Email:	Alany e-mail címe az előfizető szervezeten belül, pl. *kissj@mavinformatika.hu*	Tanúsítványigénylő űrlapnak megfelelően.

Az előfizetők tanúsítványai az Email azonosító alapján (mint keresési kulcs) a címtárban megtalálhatók.

3.1.2. Név jelentése, szemantikája

A Tanúsítványban szerepeltetendő nevek megadásánál a következő szabályok érvényesek:

- az azonosítónak értelmezhetőnek kell lenni,
- a Tanúsítványban álnév megadása lehetséges, jelölése: „~álnév~” formátumú.
- az azonosító mezőinek karaktertípusa: UTF8String,
- magyar állampolgárok nevének felvétele során a személyi igazolványba vagy az útlevélben szereplő írásmód kerül követésre, azaz a Tanúsítványba az azonosítás-hitelesítés alapjául szolgáló dokumentumban szereplő név kerül névmegadásként; ettől eltérő névmegadás álnévnek minősül,
- 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 névmegadási formák értelmezési szabályai

A névmegadási formákra vonatkozóan az 1.4.3 fejezetben meghatározott tanúsítványfajták névmegadási szabályai mérvadók.

A névmegadási formák értelmezése érdekében érintett feleknek a jelen HSzSz 1.4.3 és 3.1.1 pontjaiban leírtak alapján kell eljárniuk. Amennyiben a névmegadási formák, illetve a Tanúsítványban foglalt adatok értelmezésével kapcsolatban az Érintett félnek segítségre lenne szüksége, akkor a Szolgáltatóval közvetlenül is felveheti a kapcsolatot.

A Szolgáltató ilyen esetben az Aláíró és az Előfizető egyéb adatairól többlettájékoztatást nem ad, csak a Tanúsítványban feltüntetett adatok értelmezését segítő információt.

3.1.4. Nevek egyedisége

A Szolgáltató biztosítja címtárában a tulajdonosazonosítók egyediségét. Erről elsődlegesen az Aláíró e-mail címének a névmegadásban való szerepeltetése gondoskodik. A Szolgáltató a név azonosító kiosztásakor ellenőrzi, hogy az adott e-mail cím nem szerepel-e egy más személy részére korábban kibocsátott Tanúsítványban. Ha szerepel, és a Tanúsítvány név azonosítójának egyéb mezői sem biztosítják az egyediséget, akkor a Szolgáltató fenntartja magának a jogot a név olyan megváltoztatására, amely továbbra is jellemző az Aláíróra, de biztosítja a megkülönböztethetőséget.

A Szolgáltató biztosítja, 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 címe is szerepel, annak érdekében, hogy biztosított legyen a név megkülönböztetés, arra az esetre, ha Tanúsítvány sorozat száma és az Aláíró neve nem elég ehhez.

Amennyiben e két adat nem biztosítja a megkülönböztethetőséget, 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 ki-

osztásának 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. Védjegyek elismerésének és hitelesítésének módszere

A tanúsítványkérelemmel az Előfizető 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 vállalja 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. Az Aláírás létrehozó adat birtoklás ellenőrzésének módszere

Az 1.4 pontban meghatározott összes tanúsítvány osztály és fajta szerinti kulcspár generálása a Szolgáltató Hitelesítő Központjában 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 igazolás szükséges. A Biztonságos aláírás létrehozó eszköz személyes átvételénél az Előfizető írásban igazolja a Biztonságos aláírás létrehozó eszköz és a PIN kód átvételét. Az átvétel után az Előfizető teljes felelősséget visel a Biztonságos aláírás létrehozó eszköz és a PIN kód biztonságos használatáért és megőrzésért.

3.1.8. Személyes azonosság hitelesítése

A természetes személy Igénylőnek, illetve az igénylő szervezetnek a tanúsítványkérelemhez csatolnia kell a Szolgáltató által biztosított tanúsítványigénylő űrlapot kitöltve és aláírva, szervezeti személy tanúsítványfajta igénylés esetén a szervezet képviseletre jogosult vezető tisztségviselőinek az aláírásával ellátva.

A személyes identitást az előfizetői osztályú, természetes személy hitelesítéséhez a következő adatokat kéri az Ügyfélkapcsolati Iroda:

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

Ezen adatokat személyi igazolvány vagy útlevél személyes bemutatásával kell hitelesíteni.

Az Ügyfélkapcsolati Iroda az átadott azonosító-hitelesítő dokumentumok érvényességének és hitelességének biztonságos megállapítása érdekében kiegészítő ellenőrzést végezhet a Szolgáltató Biztonsági Szabályzatában szabályozott módon.

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 következő adatokat kéri az Ügyfélkapcsolati Iroda:

- az igénylő szervezet neve, székhelye,
- annak a szervezeti egységnek a megnevezése, ahol az Aláíró dolgozik,
- a képviseletre kijelölt Aláíró neve, aláírása,
- a képviseleti megbízás dokumentuma cégszerűen aláírva,

- annak a szervezeti egységnek a neve, e-mail címe, telefon+fax száma, amely az Aláírót megbízza,
- a képviseletre kijelölt Aláíró beosztása,
- a képviseletre kijelölt Aláíró személyi igazolvány vagy útlevél igazolvány száma,
- a képviselő Aláíró telefon száma, e-mail címe.
- az előfizető szervezet és szervezeti egység viszonya az Aláíróhoz,
- az előfizető szervezet egyértelmű hozzájárulása ahhoz, hogy:
  - a Tanúsítvány kibocsátásra kerüljön,
  - a szervezet és szervezeti egysége neve a Tanúsítvány tulajdonosazonosító mezőjében feltüntetésre kerüljön,
  - az Aláíró neve a Tanúsítvány tulajdonosazonosító mezőjében feltüntetésre kerüljön,
  - a Szolgáltató a kezdeti regisztráció során a szervezeti azonosság hitelesítésére elfogad minősített aláírással ellátott elektronikus okiratot is az Igénylőtől, abban az esetben, ha az Előfizetővel ebben előzetesen megegyezik. Ez esetben az Előfizető szervezeti azonosságának hitelesítése, s a szervezeti adatok felvétele a megegyezés során történik, az elektronikus okirat „már csak" az Előfizető hozzájárulását tartalmazza az Aláíró részére történő Tanúsítvány kibocsátásához,
  - az Előfizető kapcsolattartókat nevez meg a Szolgáltató részére, akik aláírási joggal rendelkeznek a Tanúsítvány kibocsátását illetően, a Szolgáltató később e személyeknek az aláírását fogadja el bármilyen kérelem vagy bejelentés esetén,
  - kötelezettséget vállal arra, 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 fentieken kívül még a következőket kell megadni:

- A kijelölt Aláíró 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.

Ezen adatokat a következő dokumentumokkal kell hitelesíteni:

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

Az Ügyfélkapcsolati Iroda a bemutatott iratok és okmányok érvényességét és hitelességét ellenőrzi. Szervezeti személy típusú tanúsítvány igénylés esetén az Ügyfélkapcsolati Iroda az aláírási jogosultság ellenőrzése céljából adategyeztetést végezhet a cégnyilvántartással[27].

Az Ügyfélkapcsolati Iroda szervezeti személy azonosítás-hitelesítése során köteles a Tanúsítvány kibocsátását megtagadni, amennyiben

- az okmányok személyhez vagy szervezethez tartozásával, eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel,
- 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.

3.1.9. Szervezeti identitás hitelesítése szervezeti személy tanúsítvány igénylése esetén

Az igénylő szervezetnek a tanúsítványkérelemhez csatolnia kell a Szolgáltató által biztosított tanúsítványigénylő űrlapot kitöltve, és a szervezet képviseletre jogosult vezető tisztségviselőinek az aláírásával ellátva.

A szervezeti identitást az előfizetői osztályú, szervezet hitelesítéséhez a következő adatokat kéri az Ügyfélkapcsolati Iroda:

- az igénylő szervezet neve, székhelye,
- annak a szervezeti egységnek a neve, telefon+fax száma és e-mail címe, amely az Aláírás-létrehozó eszközt és a Tanúsítványt igényli.
- az előfizető szervezet egyértelmű hozzájárulása ahhoz, hogy:

[27] 2001. évi XXXV. törvény 12. § (2) b)

- a Tanúsítvány kibocsátásra kerüljön,
- a szervezet és szervezeti egysége neve a Tanúsítvány tulajdonosazonosító mezőjében feltüntetésre kerüljön,
- az aláírói munkakör megnevezése a Tanúsítvány tulajdonosazonosító mezőjében feltüntetésre kerüljön,
- az Előfizető kapcsolattartókat nevez meg a Szolgáltató részére, akik aláírási joggal rendelkeznek a Tanúsítvány kibocsátását illetően, a Szolgáltató később e személyeknek az aláírását fogadja el bármilyen kérelem vagy bejelentés esetén,
- az előfizető szervezet kötelezettségvállalása melyben:
  - a Tanúsítvány kibocsátásával és fenntartásával kapcsolatos és minden egyéb járulékos költséget vállal,
  - a Szolgáltató szabályzataiban részletesen tárgyalt kötelezettségeit, felelősségét és jogait ismeri, s elfogadja azokat.

Ezen adatokat a következő dokumentumokkal kell hitelesíteni:

- cégbíróságnál nyilvántartott gazdasági társaságok esetében 30 napnál nem régebbi cégkivonat,
- nem cégbíróságnál nyilvántartott szervezetek esetében a nyilvántartó szervezet igazolása, pl. alapítványok esetében Fővárosi Bíróság, egyéni vállalkozók esetében az illetékes önkormányzat, ügyvédek esetében az Ügyvédi Kamara, könyvvizsgálók esetében a Könyvvizsgálói Kamara,
  igazságügyi szakértők esetében az Igazságügyi Minisztérium, stb.,
- állam-, illetve közigazgatási szervezetek esetében az alapító dokumentum közjegyzővel hitelesített másolata, amelyet a szervezet első számú vezetőjének írásos nyilatkozata kísér,
- aláírási címpéldánnyal, amely a szervezet aláírásra jogosult vezetőinek nevét és aláírását tartalmazza;
  gazdasági társaságok esetében a cégbírósági bejegyzést, más – nem gazdasági – szervezetek esetében a szervezet hivatalos bejegyzését is mellékelni kell a kérelemhez.

Az Ügyfélkapcsolati Iroda a bemutatott iratok és okmányok érvényességét és hitelességét ellenőrzi. Az Ügyfélkapcsolati Iroda az aláírási jogosultság ellenőrzése céljából adategyeztetést végezhet a cégnyilvántartással.

A Szolgáltató a kezdeti regisztráció során a szervezeti azonosság hitelesítésére elfogad minősített aláírással ellátott elektronikus okiratot is az Igénylőtől, abban az esetben, ha ebben előzetesen és írásban megegyeztek. Ez esetben az Előfizető szervezeti azonosságának hitelesítése, s a szervezeti adatok felvétele a megegyezés során történik meg, az elektronikus okirat „már csak" az Előfizető hozzájárulását tartalmazza az Aláíró részére történő Tanúsítvány kibocsátásához. A megegyezés során az Előfizető kapcsolattartókat nevez meg a Szolgáltató részére, akik aláírási joggal rendelkeznek a Tanúsítvány kibocsátását illetően.
(A Szolgáltató később e személyeknek az aláírását fogadja el a tanúsítvány kérelmen.)

Az Ügyfélkapcsolati Iroda a szervezet azonosítás-hitelesítése során köteles a Tanúsítvány kibocsátását megtagadni, amennyiben

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

3.1.10. Személyi és szervezeti identitás hitelesítése időbélyegzés szolgáltatás igénylés esetén

Időbélyegzés szolgáltatást igényelhet:

- természetes személy,
- jogi személy.

A természetes személy Igénylőnek, időbélyegzés szolgáltatás kérelemhez csatolnia kell a Szolgáltató által biztosított időbélyegzés szolgáltatás igénylő űrlapot kitöltve és aláírva.

A személyes identitás hitelesítéséhez a következő adatokat kéri az Ügyfélkapcsolati Iroda:

- Az Igénylő neve, aláírása,
- Az Igénylő okmányszáma (személyi igazolvány vagy útlevél szám),
- Az Igénylő lakcíme.

Ezen adatokat személyi igazolvány vagy útlevél személyes bemutatásával kell hitelesíteni.

Az Előfizető írásbeli nyilatkozatot ad arra vonatkozóan, hogy a Szolgáltató nyilvánosan közzétett szabályzataiban részletesen tárgyalt kötelezettségeit, felelősségét és jogait ismeri, s elfogadja azokat.

Az időbélyegzés szolgáltatási kérelem nem fogadható el, amennyiben az okmányok személyhez tartozásával, eredetiségével, valódiságával vagy érvényességével kapcsolatban kétség merül fel.

Jogi személy Igénylőnek az időbélyegzés szolgáltatás kérelemhez csatolnia kell a Szolgáltató által biztosított időbélyegzés szolgáltatás igénylő űrlapot kitöltve a szervezet képviseletre jogosult vezető tisztségviselőjének az aláírásával ellátva.

A jogi személy és a szervezet által az időbélyeg használatára felhatalmazott személy identitása hitelesítéséhez a következő adatokat kéri az Ügyfélkapcsolati Iroda:

- az igénylő szervezet neve, székhelye,
- az igénylő szervezet képviseletre kijelölt személy neve és aláírása;

  a jogi személy Igénylő kapcsolattartókat jelöl ki írásos megbízással, akik döntési és aláírási joggal rendelkeznek az időbélyegzés szolgáltatás igénybevétel során felmerülő ügyintézés vonatkozásában;

  a Szolgáltató később e személyeknek az aláírását fogadja el bármilyen kérelem vagy bejelentés esetén;

A jogi személy Igénylő kötelezettséget vállal arra, hogy a Szolgáltató nyilvánosan közzétett szabályzataiban részletesen tárgyalt kötelezettségeit, felelősségét és jogait ismeri, s elfogadja azokat.

Az azonosítás-hitelesítést támogató adatokat a következő dokumentumokkal kell hitelesíteni:

- a jogi személyt képviselő személy személyi igazolványának vagy útlevél bemutatása személyesen,
- a képviseleti megbízás dokumentuma cégszerűen aláírva,

Az Ügyfélkapcsolati Iroda a bemutatott iratok és okmányok érvényességét és hitelességét ellenőrzi. Az Ügyfélkapcsolati Iroda szervezeti személy azonosítás-hitelesítése során köteles az időbélyegzés szolgáltatást megtagadni, amennyiben

- az okmányok személyhez vagy szervezethez tartozásával, eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel,
- a bemutatott iratok és okmányok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel,
- a képviselő szervezethez tartozása nem egyértelmű,
- a szervezet kiléte nem állapítható meg minden kétséget kizáróan.

Az időbélyegzés szolgáltatás igénybe vételekor a Szolgáltató az igénybe vevőnél biztonságos csatornán keresztüli tanúsítvány alapú kliens azonosítást alkalmaz. Ehhez érvényes, HIF által regisztrált hitelesítés szolgáltató által kibocsátott, azonosítás-hitelesítésre alkalmas Tanúsítvány szükséges[28].

3.2. Érvényes Tanúsítvány megújítás (Tanúsítvány frissítés)

Egy érvényes (nem lejárt és nem visszavont) Tanúsítvány *frissítésére* akkor kerül sor, amikor a Szolgáltató érvényes magánkulcsával az új Tanúsítványban a Tanúsítvány Tulajdonosának változatlan (régi) nyilvános kulcsát és változatlan egyéb adatait írja alá új érvényességi időtartamra.

Tanúsítványának lejárta előtt, az Előfizető az Előfizetői Szerződésben meghatározott időpontban (ha a Szerződés erről nem intézkedik, akkor a lejárat előtt 14 nappal korábban) e-mailben kap értesítést a Szolgáltatótól a tanúsítvány frissítés szükségességéről.

Az Előfizető értesítése után a Tanúsítvány lejártakor a Szolgáltató a Tanúsítvány érvényességi idejét 1 évre meghosszabbítja feltéve, ha az Előfizető az értesítés után ez ellen nem emel kifogást.

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

Előfizetői tanúsítvány frissítése akkor lehetséges, ha:

- a Tanúsítvány érvényes,

[28] Magyarország EU tagságától kezdve bármely, az EU-ban regisztrált hitelesítés szolgáltató által kibocsátott, azonosítás-hitelesítésre alkalmas Tanúsítvány megfelel.

- 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, hogy 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 megújítása

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 és 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 igénylésével történik, a regisztrációs eljárás 3.1.8 és 3.1.9 pontok szerinti végrehajtásával.

3.4. Felfüggesztés és visszavonás kérés

Visszavonási kérés csak személyes megjelenéssel történhet. Az Előfizetőnek, illetve az Aláírónak lehetősége van a Tanúsítvány felfüggesztését kérni telefonon (az ilyenkor szükséges jelszó megadása mellett) vagy elektronikusan aláírt e-mail-ben. Indokolt esetben harmadik fél is kérheti a Tanúsítvány felfüggesztését, de kizárólag személyesen.

A tanúsítvány visszavonási kérés azonosítás-hitelesítési vonatkozásai megtalálhatóak a 4.5 fejezetben.

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 4.5

pont 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 követelmények,
- milyen okból kifolyólag függeszthető fel egy Tanúsítvány,
- mi a felfüggesztett állapot maximális időtartama.

4. A működésre vonatkozó követelmények

4.1. Tanúsítványigénylés

Tanúsítvány a Szolgáltatótól az Ügyfélkapcsolati Irodánál igényelhető, az adott tanúsítvány osztálynak és az MTT, illetve az MTT+BALE típusnak megfelelő, a 3.1.8 és a 3.1.9 pontokban meghatározott azonosítás-hitelesítési feltételek mellett, a regisztrációs eljárás lefolytatásával.

a. A Szolgáltatónak azt megelőzően, hogy egy Előfizetővel szerződéses kapcsolatot létesít, tájékoztatnia kell az Előfizetőt a Tanúsítvány és/vagy az időbélyeg használatával kapcsolatos kikötésekről és feltételekről a 2.6.1 pontban megadottak szerint. A kapcsolatfelvételkor – amennyiben az Igénylő Aláírás létrehozó adat és eszköz használati igényét egyértelműen jelzi – Tanúsítvány űrlapot kap az Ügyfélkapcsolati Iroda munkatársától.

b. A Tanúsítvány űrlap átvételét követően a Szolgáltató tájékoztatási kötelezettségét tájékoztató kiadványnak (Tájékoztató, ÁSzF) az Igénylő részére történő átadásával teljesíti. Igénylőnek módja van e dokumentumok helyszínen történő áttanulmányozására és helyszíni konzultációra, de azok, valamint a Tanúsítvány igénylő űrlap megtalálható szolgáltató honlapján is, így előzetesen is áttekinthető[29] és kitölthető. Amennyiben az Előfizető igényli, az Ügyfélkapcsolati Iroda az egyéb nyilvános dokumentumok tanulmányozásának lehetőségét is biztosítja, valamint szóban válaszol az Igénylő, a szerződéskötéssel kapcsolatos további kérdéseire.

   A Tájékoztató tartalma:

   - A HSzSz-nek az Előfizető szempontjából legfontosabb szabályokat, feltételeket tartalmazó kivonata, (természetesen az Igénylő az Ügyfélkapcsolati Iroda által megadott elérhetőségen a HSzSz-t teljes egészében is elolvashatja).
   - A Szolgáltató további nyilvános dokumentumainak szerepe és elérhetősége.
   - Egyéb technikai eligazítás.

[29] Az űrlap a regisztrációs adatok mellett tartalmazza a szükséges nyilatkozatokat és igénylő fizikai címét, illetve más jellemzőit, amelyek leírják, hogy hogyan lehet felvenni vele a kapcsolatot.

c. A Szolgáltató az Aláírót is tájékoztatja kötelességeiről.
d. 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.
e. A személyes és szervezeti identitások hitelesítése, űrlapon szereplő adatok formai és tartalmi ellenőrzése.

   A személy- és szervezeti azonosság, valamint a szervezethez tartozás megállapítása a 3.1.8 és 3.1.9 fejezetekben leírtak alapján történik. Amennyiben az azonosság nem állapítható meg minden kétséget kizáróan, vagy valamely az űrlapon feltüntetett adat nem helyes, akkor az igénylési eljárás félbeszakad. Szolgáltató az űrlapot visszaadja igénylő részére, akinek lehetősége van az adatok korrigálására, s újbóli igénylésre.
f. A regisztrációhoz szükséges dokumentumok és adatok formai és tartalmi ellenőrzése után a regisztrációt végző személy ellenőrzi a regisztrációs űrlapon szereplő adatok egyezőségét az Előfizető dokumentumaiban szereplő adatokkal.
g. Ha az adatok helyesek, az űrlap tartalmát rögzíti az Ügyfélkapcsolati Iroda informatikai rendszerében, ellenkező esetben az űrlapot visszaadja.
h. Az Aláíró azonosítójának (egyedi nevének) megállapítása a 3.1.1 pontban tárgyaltaknak megfelelően.
i. Az Előfizetői szerződés megkötése a Szolgáltató előfizetői szerződés mintájának megfelelően. Az Igénylő aláírásával Előfizetővé válik és egyúttal nyilatkozik arról is, hogy a Szolgáltató feltételei és kikötései, saját kötelezettségei vonatkozásában tájékoztatást kapott, azokat elfogadja. Az aláírással az Előfizető hozzájárul a szolgáltatások során felhasznált információknak a Szolgáltató által történő nyilvántartásba vételéhez, Tanúsítványa és az azzal kapcsolatos állapot információ szolgáltatói címtárban való közzétételéhez, s ezen információ harmadik félhez történő továbbításához a Szolgáltató szolgáltatásainak leállítása esetén, illetve egyéb jogszabályok által meghatározott esetekben, a Szolgáltató szabályzatai által meghatározott módon.

   Az Előfizető aláírása igazolja azt is, hogy az Előfizető:
   - vállalja MTT+BALE típusú tanúsítvány kiadása esetén a Biztonságos aláírás-létrehozó eszköz használatát, védelmét,
   - vállalja MTT típusú tanúsítvány kiadása esetén az Aláírás-létrehozó eszköz használatát, védelmét,

- garantálja feltüntetett adatainak valódiságát,
- az adatok későbbi változásairól a Szolgáltatót értesíti.

j. Az Ügyfélkapcsolati Iroda nyilvántartásba vesz minden, az Aláíró azonosságának igazolására használt információt, beleértve az igazoláshoz használt dokumentáció regisztrációs számát és az annak érvényességével kapcsolatos esetleges korlátozásokat. A dokumentációkról az Ügyfélkapcsolati Iroda másolatot készít.

k. A Tanúsítványigénylő űrlap tartalmát az Ügyfélkapcsolati Iroda nyilvántartásába veszi és archiválásra kerül mind elektronikus, mind papír formában.

l. Az Ügyfélkapcsolati Iroda nyilvántartásba veszi az Előfizetővel aláírt nyilatkozatokat[30] és, beleértve az alábbiakat:

- az Előfizető kötelezettségeivel (lásd 2.1.7) történő egyetértést,
- az Előfizető beleegyezését a Biztonságos aláírás-létrehozó eszköz használatára vonatkozóan,
- 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 HSzSz által megkövetelt feltételek szerint),
- hogy az Előfizető megköveteli-e, az Aláíró pedig hozzájárul-e a Tanúsítvány közzétételéhez és milyen feltételek mellett,
- annak megerősítését, hogy a Tanúsítványban szereplő információ helyes[31].

A Szolgáltató megőrzi a d)-f) pontokban megnevezett nyilvántartásokat 10 évig[32], illetőleg a velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig.

Sikeres regisztráció után az Ügyfélkapcsolati Iroda a tanúsítvány igényt a Regisztrációs Iroda felé továbbítja, amellyel elbírálási igényt támaszt a fölérendelt Hitelesítő Központ felé. A Regisztrációs Iroda a kedvező elbírálás után a hitelesítés szolgáltatást támogató informatikai rendszerbe a tanúsítvány kibocsátási igényt beviszi.

[30] 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.

[31] A fenti megállapodás elektronikus formát is ölthet.

[32] A 2001. évi XXXV. törvény 9. § (7) pontja legalább 10 év megőrzési időt követel meg.

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.

Időbélyegzés szolgáltatás igénylése esetén az Igénylőt a jelen pontban ismertetett módon tájékoztatni kell az időbélyeg használat módjáról az azzal járó kötelezettségekről és felelősségről.

Az Igénylő azonosítását a 3.1 pontban leírt egyszerűsített eljárással kell elvégezni.

4.2. Tanúsítvány kibocsátás

Az elkészült Tanúsítványt a Szolgáltató a következő módon juttatja el az Előfizetőhöz:

- az Előfizető, az Aláíró vagy az eredetileg regisztrált képviselője személyesen átveheti az Ügyfélkapcsolati Irodán, vagy utólagosan letöltheti a nyilvános Címtárból (MTT),
- a Szolgáltató a Biztonságos aláírás-létrehozó eszközön juttatja el az Aláíróhoz vagy az Előfizetőhöz (MTT-BALE).

A Szolgáltató biztonságosan fenntartja az általa kibocsátott tanúsítványok hitelességét következő módokon:

- 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 során:
  - a Tanúsítvány kibocsátás eljárása biztonságosan kapcsolódik a Szolgáltató általi kulcspár előállításhoz,
  - az Aláíró Aláírás létrehozó adatát tartalmazó Biztonságos aláírás létrehozó eszközt biztonságosan juttatják el az Előfizetőhöz,

- 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 újít meg egy Tanúsítványt ily módon.

A Hitelesítő Központ csak akkor fogadja el a tanúsítványkérelmet, ha a következő feltételek teljesülnek:

- az Aláíró benyújtotta kérelmét az Ügyfélkapcsolati Irodának,
- az Aláíró azonos a kérelemben szereplő alannyal (subject),
- az Igénylő jogosult a kérelemben szereplő Aláíró nevében kérelmet benyújtani,
- az Ügyfélkapcsolati Iroda 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 az Ügyfélkapcsolati Iroda által felvett elektronikus űrlap alapján végzi a Hitelesítő Központ.

A Hitelesítő Központ az előállított Tanúsítványt visszaküldi az Regisztrációs Irodához. Amennyiben a tanúsítványkérelem visszautasításra kerül ennek tényéről és okáról az Regisztrációs Iroda értesítést kap.

4.3. Időbélyeg kibocsátás

Az időbélyegzés szolgáltatás megkezdése a regisztrált időbélyeg felhasználó fél részére a szerződéskötést követően 24 órán belül megkezdődik. Az időbélyegzés kérelmek fogadása, ellenőrzése és kibocsátását az időbélyegző központ automatikusan végzi.

Az időbélyegzés szolgáltatást a Szolgáltató a Trust&Sign® Időpecsételés Szolgáltatás márkanév alatt nyújtja a regisztrált ügyfelei számára.

Ez a szolgáltatás két részből tevődik össze:

1. A szolgáltatás igénybevételét egy olyan HTTPS (https://tsa.trust-sign.hu:1318 című) kommunikációs csatornán keresztül lehet kérni, melynek publikus kliens kulcsa megegyezik a regisztráció során megadott publikus kulccsal.
2. Az időbélyeg kérés kiszolgálása az RFC 3161 ajánlás szerinti „application/timestamp-query" MIME-TYPE elküldésére valósul meg.

Az időbélyeg kibocsátás minőségét a következő jellemzők határozzák meg:

- Az időbélyegben megadott idő pontossága.
  - Az időbélyegző szerver belső óráját egy 1 másodpercnél nagyobb pontosságú, négy egymástól független, külső UTC időforrás által szinkronizált másik belső óra szinkronizálja, így az ISzP által előírt 1 másodpercen belüli pontosság biztosított.
  - Az időbélyegző szerver belső órájának pontossága folyamatos ellenőrzés alatt áll. Amennyiben az óra pontossága túllépné az előírt pontossági határt, az ellenőrző program leállítja az időbélyegzés szolgáltatást, és minden további kérésre a hiba kijavításáig hibaüzenetet küld a felhasználók felé.
  - A szolgáltatás akkor indul újra, ha egymásután két, a pontossági határon belül eső időszinkront kap a belső óra. Ez az időszinkron helyreállása után maximálisan húsz percet vehet igénybe.
- Az időbélyegző szerver belső óra szinkronizálásának pontossága.
- A szinkronizáló időalap magas rendelkezésre és állása hitelessége.
  - Az időbélyegző központ óráját négy egymástól független UTC időjelből képzett szinkron órajel szinkronizálja. Ez biztosítja az időbélyegző szerver belső órája szinkronizálásának pontosságát.
  - Amennyiben az egyik UTC időalap szolgáltató órájának pontossága az előírt határon kívül kerül, akkor a szinkronizáció automatikusan a tartalék időalap forrásokból képzett szinkron órajellel történik.
  - A szinkronizáló UTC időjelek hitelességét az időbélyegző rendszer indításánál az erre a célra létrehozott bizottság tanúsítja.

- Amennyiben üzem közben a hitelesség sérülésének vagy elvesztésének komoly gyanúja áll fenn, a bizottság összehívásra kerül, elvégzi a szinkronizáló UTC időjelek ellenőrzését és egy független GSM kapcsolaton keresztül lekérdezett UTC időt referenciaként használva állást foglal a szinkronizáló időforrások hitelességét illetően.

♦ Az időbélyegzés szolgáltatás rendelkezésre állása.
  - Az időbélyegző szolgáltatásnak az ISzP-ben meghatározott rendelkezésre állási szintje 99,5%. Ez a követelménynek a kielégítése a meleg tartalékolt időbélyegző szerver architektúrával, és a szervereknek a hitelesítés szolgáltató informatikai rendszer magas rendelkezésre állást (high availability /HA/) felügyelő és vezérlő rendszerébe történő integrálásával biztosított.

♦ Aláíró kulcs fokozott biztonságú védelme kompromittálódás ellen.
  - Az időbélyeg aláíró kulcspár generálását és az aláíró kulcs biztonságos tárolását a 2/2002. (IV. 26.) MeHVM irányelv 212. pontjában előírt tanúsítással rendelkező HSM egység végzi.
  - Az időbélyegző szerverek és a HSM egység többszörös tűzfal rendszer védi a külső hálózatokról érkező fenyegetésektől. Fizikai védelem szempontjából a Bizalmi Központban történt elhelyezés biztosítja a fokozott védelmet.

4.4. Tanúsítvány elfogadás

A Regisztrációs Iroda, a Szolgáltató felelősségi körében eljárva az elkészült Tanúsítványt ellenőrzi, Biztonságos aláírás létrehozó eszközre írja az Aláírás létrehozó adattal együtt, majd a Bizalmi Központ munkatársai eszközt és a PIN kódot egymástól elkülönítve eljuttatatják az Ügyfélkapcsolati Irodába, ahol azok a személyesen megjelent Előfizetőnek, Aláírónak vagy az eredetileg regisztrált képviselőnek átadásra kerülnek. A PIN kód kinyomtatása után biztonságos postázással (futárral vagy tértivevényes postázással) is eljuttatható az Előfizetőhöz.

Előfizetői szerződés megkötése után átadásra kerül:

♦ az Aláírás létrehozó adat és a Tanúsítvány,

♦ a PIN kód, (amennyiben nem postázás útján lesz az Aláíróhoz eljuttatva),

♦ a felfüggesztési jelszó,

♦ az aláírt tanúsítvány igénylő űrlap egy eredeti példánya,

- a Tájékoztató,
- az aláírt Előfizetői Szerződés egy példánya.

Az Aláírás-létrehozó eszköz átvételének megtagadása visszavonási kérelemnek számít.

Amennyiben a regisztrációs eljárás és a Biztonságos aláírás létrehozó eszköz átadása között az Előfizetővel a személyes kapcsolat megszakadt, az Előfizető személyazonosságát újra ellenőrizni kell a Biztonságos aláírás létrehozó eszköz átadása előtt.

A személyes átadásnál az Aláírás-létrehozó eszközt kizárólag a regisztrációs űrlapon megjelölt Aláíró vagy az eredetileg regisztrált képviselő veheti át.

Az Aláírás létrehozó adat és a Tanúsítvány elfogadása az Aláírás létrehozó adat első felhasználásával történik meg.

Az Aláírás létrehozó eszköz átvételekor az Előfizetőnek írásban kell megerősíteni a következőket:

- ismeri, érti és elfogadja a Szolgáltató jelen és kapcsolódó nyilvánosan hozzáférhető szabályzatait,
- minden adat, amit a Szolgáltatónak a Tanúsítvány kiadásának céljából átadott, a valóságnak megfelel és azok átadása önkéntes volt,
- a Tanúsítványban szereplő minden adat az Előfizető tudomásával és egyetértésével került a Tanúsítványba,
- a Tanúsítvány érvényességét befolyásoló tényekről haladéktalanul értesíti a Szolgáltatót,
- mindent megtesz annak érdekében, hogy jogosulatlan személy nem férjen hozzá az Aláírás létrehozó adathoz,
- ismeri az elektronikus aláírás megfelelő használatának módját, tisztában van az elektronikus aláírás használatának technikai feltételeivel és jogi következményeivel,
- minden egyes elektronikus aláírást, amely a Tanúsítványban szereplő Aláírás ellenőrző adat párjával, azaz az Aláírás létrehozó adattal készült, az Aláíró saját elektronikus aláírásának ismeri el,
- tudomással bír arról, hogy az elektronikus aláírással ellátott elektronikus iratok az írásbafoglalás jogszabályi követelményének megfelelnek,
- minden aláírás az elfogadott és érvényes (vissza nem vont, nem lejárt) Tanúsítvány alapján készült,

- a Tanúsítványt kizárólag törvényes célokra, jogszerűen, a jelen és kapcsolódó szabályzatoknak és törvényi előírásoknak megfelelően használja,
- tisztában van azzal, hogy az Aláírás létrehozó adat védelme és az elektronikus aláírás készítése kizárólag a Felhasználó felelőssége, s ezzel kapcsolatban a Szolgáltatót semmiféle felelősség nem terheli,
- az Aláíró végfelhasználó, azaz nem hitelesítés szolgáltató, és nem fogja a Tanúsítványban megadott Aláírás ellenőrző adat párját, azaz az Aláírás létrehozó adatot újabb tanúsítványok vagy bármely más formátumú tanúsított Aláírás ellenőrző adat, visszavonási lista kiadására használni,
- felhatalmazza a Szolgáltatót a Tanúsítvány nyilvánosságra hozatalával, és saját vagy más nyilvános Címtárakban történő elhelyezésével.

Az Aláírás létrehozó adat használatba vétele előtt az Előfizetőnek kötelessége ellenőrizni a Tanúsítványban feltűntetett adatainak helyességét. Amennyiben bármilyen rendellenességet talál, az Aláírás létrehozó adat nem használhatja fel, hanem azonnal intézkednie kell a Tanúsítvány visszavonása érdekében.

A Szolgáltató elutasítja a tanúsítványkérelmeket, ha az azonosítás-hitelesítési és regisztrációs feltételek a jelen HSzSz szerint nem biztosíthatók az igényelt Tanúsítvány típusának, osztályának és fajtájának előírt módon.

Az elutasított kérelmekről az Igénylő írásbeli értesítést kap, melyben szerepel az elutasítás indoka. Amennyiben az elutasítás oka harmadik fél által szolgáltatott információ, az értesítés megnevezi az elutasítást eredményező információforrást is.

Elutasítás után a kérelmező új kérelemmel fordulhat a Szolgáltatóhoz.

4.5. 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 4.5.8 pont) után állapotát újra érvé-

nyesre kell állítani, vagy vissza kell vonni. A felfüggesztett Tanúsítvány mindaddig, amíg felfüggesztett állapotban van, ugyanúgy érvénytelenként kezelendő, mint a visszavont.

A visszavont/felfüggesztett Tanúsítványhoz tartozó Aláírás létrehozó adat használatát azonnal meg kell szüntetni, illetve fel kell függeszteni. A visszavont Tanúsítványhoz tartozó Aláíró létrehozó adatot, illetve eszközt a visszavonást követően azonnal meg kell semmisíteni. A megsemmisítéséig az Aláíró létrehozó adat, illetve eszköz ugyanolyan felügyeletben részesítendő, mintha érvényes lenne.

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

4.5.1. Visszavonáshoz vezető körülmények

Az Előfizető, az Aláíró vagy az eredetileg regisztrált képviselő a következő körülmények fennállása esetén kezdeményezi a visszavonást:

- a magánkulcs kompromittálódása, vagy annak gyanúja,
- a Biztonságos aláírás-létrehozó eszköz elvesztése, eltulajdonítása, megrongálódása,
- a Biztonságos aláírás-létrehozó eszközt védő aktivizáló adat (PIN kód) kompromittálódása, vagy annak gyanúja,
- a magánkulcs átvételének visszautasítása,
- a Tanúsítványban feltűntetett hibás adatok,
- az Előfizetőnek a Tanúsítványban feltűntetett adatainak megváltozása,
- az Aláírónak a Tanúsítványban feltűntetett adatainak megváltozása,
- a Tanúsítványban feltűntetett szervezet adatainak megváltozása,
- a Tanúsítványban feltűntetett Aláíró és szervezet kapcsolatának megváltozása vagy megszűnése[33].

miatt.

Visszavonási kérelmet mérlegelés nélkül teljesíteni kell, ha az Aláíró, az Előfizető vagy a kezdeti regisztráláskor nyilvántartásba vett képviselő kéri.

[33] A 2001. évi XXXV. törvény 10. § (3)

A Szolgáltató kezdeményezése alapján:

- a Tanúsítvány felfüggesztési idejének lejárata,
- amennyiben a törvény erre kötelezi,
- az ÁSzF, Előfizetői Szerződés megszegése az Előfizető és/vagy az Aláíró által,
- az Előfizető és/vagy az Aláíró kötelezettségeinek be nem tartása,
- az Előfizetői szerződés megszűnése,
- a Szolgáltató tudomására jutott tény, vagy alapos gyanú, a regisztrációs adatok valótlanságáról,
- a Tanúsítványban feltűntetett kibocsátó adatok megváltozása
- a hitelesítési szolgáltatás megszűnése,
- a Regisztrációs Iroda megszűnése,
- a Szolgáltató valamely magánkulcsának kompromittálódása

miatt.

Harmadik fél, pl. Érintett fél kezdeményezése alapján.

Egyéb visszavonáshoz vezető körülmények:

- az Aláíró halála, az Előfizető megszűnése,
- jogszabály kötelező ereje.

4.5.2. Visszavonás kérelmezése

Tanúsítvány visszavonását az előző pontban feltüntetett körülmények alapján az Előfizető, annak a kezdeti regisztrációkor nyilvántartásba vett képviselője, a Szolgáltató, hatósági szervezet vagy más harmadik fél kezdeményezheti. Az Előfizetőnek és Szolgáltatónak kötelessége, harmadik félnek joga, a feltűntetett esetekben a visszavonás azonnali kezdeményezése.

A visszavonási kérelmet csak személyesen és írásban a Szolgáltató Ügyfélkapcsolati Irodánál lehet benyújtani vagy az Ügyfélszolgálatnál (Help Desk) lehet bejelenteni.

Amennyiben a bejelentő akadályoztatása miatt a visszavonási igényét személyesen nem tudja bejelenteni, akkor telefonon vagy elektronikusan aláírt e-mail-ben a Tanúsítvány felfüggesztését kérheti (lásd 4.5.6 pont!) és az ettől számított 30 napon belül megteheti a visszavonás személyes bejelentését.

A visszavonási kérelemnek a következő adatokat kell tartalmazni:

- a Tanúsítvány sorszáma,
- a visszavonást kérő megnevezése,
- a visszavonást kérő e-mail címe,
- a visszavonás oka.

4.5.3. Visszavonási eljárás

A visszavonási eljárás első lépéseként a Szolgáltató Ügyfélkapcsolati Irodája vagy a munkaidőn kívül az Ügyfélszolgálat (Help Desk) azonosítja a bejelentőt, aki lehet:

- természetes személy Előfizető esetén maga az Aláíró vagy az általa megbízott és a Szolgáltató által nyilvántartott képviselője,
- jogi személy Előfizető esetén maga az Aláíró vagy a jogi személy által megbízott és a Szolgáltató által nyilvántartott képviselő.

Az Ügyfélkapcsolati Irodánál az Iroda munkaidején belül bejelentett visszavonási kérelmeket a bejelentő azonosítása-hitelesítése, valamint a visszavonási kérelem formai és tartalmi ellenőrzése után haladéktalanul a Hitelesítő Központhoz kell továbbítani, amely azokat ismét ellenőrzi.

Az Ügyfélkapcsolati Iroda munkaidején kívül a telefonon jelentkező bejelentőt Help Desknél az erre feljogosított munkatárs azonosítja, valamint a kérelmet formailag és tartalmilag ellenőrzi. Amennyiben az ellenőrzések pozitív eredménnyel zárulnak, a feljogosított ügyeletes a Tanúsítvány felfüggesztését és közzétételét elvégzi. A visszavonás kérelmezése ténylegesen az Ügyfélkapcsolati Irodában személyes megjelenés útján, legkésőbb 30 napon belül, a bejelentő megnyugtató azonosítás-hitelesítését követően fog megtörténni.

Ha az okok nem megalapozottak, az adatok helytelenek, vagy a kérelmező személye nem állapítható meg, akkor a Szolgáltató a visszavonási kérelmet visszautasítja.

A visszavont Tanúsítvány bekerül a következő alkalommal kibocsátott Tanúsítvány visszavonási listába.

Szolgáltató a visszavonás megtörténtéről vagy visszautasításáról elektronikusan aláírt e-mailben értesíti az Előfizetőt és a visszavonás kérelmezőjét.

A Szolgáltató nem állítja vissza érvényesre a már egyszer véglegesen visszavonásra került tanúsítványokat.

Előfizetői tanúsítvány visszavonását és felfüggesztését a Szolgáltató akkor is nyilvánosságra hozza, ha a Tanúsítvány közzétételéhez az Előfizető nem járult hozzá.

4.5.4. Visszavonási/felfüggesztési kérelemre vonatkozó türelmi idő

A visszavonási/felfüggesztési kérelem esetén a bejelentési kötelezettség azonnali, a Szolgáltató a kérelmet soron kívül végrehajtja annak elfogadása után. A legnagyobb késedelem a visszavonási/felfüggesztési 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/felfüggesztése esetén a Tanúsítványt a továbbiakban joghatályosan nem lehet felhasználni.

A Szolgáltatót és az Előfizetőt érintő felelősségi szabályok:

- A visszavonási/felfüggesztési kérelem bejelentésének a Szolgáltatóhoz történő megérkezéséig az ÁSzF-nek megfelelően az Előfizető felelős a felmerülő károkért.
- A visszavonási/felfüggesztési kérelem megérkezésétől a visszavonás/felfüggesztés tényének Címtárban való megjelenésig a Szolgáltató felelős a felmerülő károkért.
- A visszavonás/felfüggesztés Címtárban való megjelenése után az Érintett fél felelős a felmerülő károkért.

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

4.5.5. Felfüggesztéshez vezető körülmények

Az Előfizető, az Aláíró vagy az eredetileg regisztrált képviselő a következő körülmények fennállása esetén kezdeményezi a felfüggesztést:

- a magánkulcs kompromittálódásának gyanúja,
- a Biztonságos aláírás-létrehozó eszköz elvesztése, eltulajdonításának gyanúja,
- a Biztonságos aláírás-létrehozó eszközt védő aktivizáló adat (PIN kód) kompromittálódásának gyanúja,

miatt.

A felfüggesztési kérelmet mérlegelés nélkül teljesíteni kell, ha az Aláíró, az Előfizető vagy a kezdeti regisztrációkor nyilvántartásba vett képviselő kéri.

A Szolgáltató a regisztrációs adatok valótlanságának alapos gyanúja esetén kezdeményezheti a felfüggesztést. Mindenképpen meg kell győződnie a gyanú alaposságáról, illetve alaptalanságáról és ennek függvényében kell dönteni a Tanúsítvány visszavonásáról.

Harmadik fél kezdeményezése alapján, amikor a Tanúsítvány hitelességével kapcsolatosan kétely vagy alapos gyanú merül fel.

Általános szabály az, hogy a Szolgáltató egy Tanúsítvány hitelességével kapcsolatosan felmerülő kétely vagy a hitelesség sérülésének alapos gyanúja esetén, dönthet a Tanúsítvány felfüggesztéséről. Ilyen esetekben a Szolgáltatónak a felfüggesztett állapot időtartama alatt intézkednie kell a körülmények tisztázása, s szükséges esetén a Tanúsítvány visszavonása érdekében. Tanúsítvány felfüggesztését harmadik fél is kérheti, amennyiben bizonyítani tud olyan körülményt, mely alapján Előfizetőnek vagy Szolgáltatónak kezdeményeznie kellene a visszavonást.

Amennyiben az Előfizető kötelessége a Tanúsítvány visszavonásának kérelmezése, de személyes megjelenése akadályoztatva van, vagy nem lehetséges, akkor haladéktalanul intézkednie kell Tanúsítványának felfüggesztése érdekében.

4.5.6. Felfüggesztés kérelmezése

A Tanúsítvány felfüggesztésére vonatkozó kérelem a következő módokon nyújtható be a Szolgáltatónak:

- elektronikusan aláírt e-mail írásával, a küldő, a Tanúsítvány azonosításához szükséges adatok, és a felfüggesztést indokoló okok feltüntetésével,
- személyes megjelenéssel az Ügyfélkapcsolati Irodánál,
- az Ügyfélszolgálat (Help Desk) telefonszámán.

A telefonon keresztül történő bejelentésénél a bejelentőt a felfüggesztési jelszóval kell hitelesíteni.

A felfüggesztési kérelemnek a következő adatokat kell tartalmazni:

- a Tanúsítvány sorszáma,
- a felfüggesztést kérő megnevezése,
- a felfüggesztési jelszó,
- a felfüggesztést kérő e-mail címe,
- a felfüggesztés oka.

Harmadik fél[34] csak személyesen vagy elektronikus aláírással ellátott e-mailben kérheti egy Tanúsítvány felfüggesztését. A felfüggesztési jelszó megadása harmadik fél számára nem kötelező, de meg kell adnia a személyes adatait is (lakcím, személyi igazolvány vagy útlevél száma), s személyes megjelenés esetén a személyazonosságát is igazolnia kell. Elektronikusan aláírt e-mail esetén a kérelmező Tanúsítványa és személyazonossága leellenőrizendő.

4.5.7. Felfüggesztési eljárás

A felfüggesztési eljárás első lépéseként Szolgáltató azonosítja és hitelesíti a bejelentőt, majd ellenőrzi a kérelemben szereplő okokat és a kérelmező adatait. Amennyiben azok helytelenek, a kérelem nem megalapozott, vagy a kérelmező személye nem megállapítható, akkor Szolgáltató a felfüggesztési kérelmet visszautasítja.

[34] Harmadik félként kell tekintetbe venni, például az Érintett felet, jogi, állam- vagy közigazgatási eljárás keretében eljáró hatóságot, stb.

Amennyiben a kérelmet az Előfizető terjesztette be, a sikeres ellenőrzés után a Szolgáltatónak nincs mérlegelési joga a végrehajtás tekintetében.

A bejelentett felfüggesztési kérelmeket az Ügyfélkapcsolati Iroda a Regisztrációs Irodához továbbítja az Ügyfélkapcsolati Iroda munkaidején belül. Azon kívül az Ügyfélszolgálat feljogosított ügyeletese elvégzi a bejelentő és a bejelentés ellenőrzését és annak sikeres befejezése esetén elvégzi a Tanúsítvány felfüggesztését és a felfüggesztés közzétételét.

Szolgáltató a felfüggesztés megtörténtéről, vagy visszautasításáról elektronikusan aláírt e-mail-ben értesíti az Előfizetőt és a felfüggesztés kérelmezőjét.

A felfüggesztési kérelem bejelentésének és végrehajtásának az Aláírás létrehozó adat kompromittálódása esetén az észlelést követően, késlekedés nélkül, minden más műveletet megelőzve meg kell történnie.

4.5.8. A felfüggesztett állapotra vonatkozó korlátozások

Legfeljebb 30 naptári napig lehet egy Tanúsítvány felfüggesztett állapotban. Ez az időszak áll rendelkezésre, hogy a Szolgáltató döntsön a Tanúsítvány állapotáról.

Amennyiben Szolgáltató kérte a felfüggesztést és nem képes ezen időszak alatt a körülmények kivizsgálására, akkor a Tanúsítványt visszavonja. Az Előfizető igénye estén részére új Tanúsítványt bocsát ki térítésmentesen.

Ha a felfüggesztést az Előfizető, vagy a Tanúsítványban feltüntetett szervezet kérte, akkor a kérelmezőnek ezen időszak alatt értesítenie kell a Szolgáltatót a Tanúsítvány érvényesítése vagy visszavonása felől. Ha ilyen értesítés nem történik, a Szolgáltató a Tanúsítványt minden mérlegelés nélkül visszavonja.

A felfüggesztés megszüntetése az időszak vége előtt is kérvényezhető. A felfüggesztés megszűntetésének eredménye vagy a Tanúsítvány újra érvényesítése vagy annak visszavonása lehet.

A felfüggesztés megszüntetésének feltételei a következők:

- A felfüggesztést megszüntetését kérheti ugyanaz a személy kérheti az Aláíró, az Előfizető vagy a kezdeti regisztrációkor nyilvántartásba vett képviselője,

- csak személyes megjelenés keretében eszközölhető a felfüggesztés megszüntetésének kérelmezése,
- a felfüggesztés megszüntetését kérő személyt azonosítani és hitelesíteni kell, ennek során kérni kell tőle a felfüggesztési jelszót.

A felfüggesztés megszüntetésének kéréséhez a következő adatokat kell megadni:

- a felfüggesztett Tanúsítvány sorszáma,
- a felfüggesztés megszüntetést kérő megnevezése,
- a felfüggesztést megszüntetést kérő e-mail címe,
- a felfüggesztés megszüntetés kérés oka.

4.5.9. CRL kibocsátás gyakorisága

A Szolgáltató Tanúsítvány visszavonási listát legalább 24 óránként bocsát ki. A Tanúsítvány visszavonási listában megadja a Visszavonási lista érvényességi idejét. Tanúsítvány visszavonási lista a megjelölt tervezett idő előtt is kibocsátható.

A visszavonási listában a visszavont és felfüggesztett tanúsítványok kerülnek feltüntetésre. A felfüggesztett tanúsítványok az újbóli érvényesítés hatására kerülhetnek ki a listából. Visszavont tanúsítványok a Tanúsítvány lejárta után 1 évvel törlődnek a listából.

A visszavonási lista elérhetőségét a Szolgáltató minden nap 24 órában, 99,9%-os rendelkezésre állással biztosítja úgy, hogy az esetenkénti elérhetőség kiesés nem lehet több, mint 3 óra.

4.5.10. CRL ellenőrzési követelmények

A Visszavonási lista ellenőrzése az érintett felek részére kötelező a tanúsítványok elfogadását megelőzően. A Tanúsítványhoz tartozó visszavonási lista elérhetőségét a Tanúsítvány tartalmazza. A lista ellenőrzésének arra kell vonatkozni, hogy a kérdéses Tanúsítványt a lista tartalmazza-e, a lista hiteles és sértetlen, s a kérdéses tranzakció szempontjából időben releváns-e.

A Tanúsítvány visszavonási listában a Szolgáltató által közzétett érvénytelen, vagy felfüggesztett Tanúsítvány elfogadásából keletkező bárminemű kár Érintett felet terheli. Lásd még a 2.2.8 pontot!

A Szolgáltató megvédi a Tanúsítvány visszavonási lista sértetlenségét és hitelességét.

4.5.11. On-line visszavonási státusz-szolgáltatás

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

4.5.12. On-line visszavonás ellenőrzési követelmények

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

4.5.13. 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.

4.5.14. Visszavonási állapot közlés más formáinak ellenőrzési követelményei

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

4.5.15. Az Aláírás létrehozó adat 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 Aláírás létrehozó adat tovább nem használható. A kompromittálódott Aláírás létrehozó adat, illetve eszköz a megsemmisítéséig ugyanolyan felügyeletben részesítendő, mint egy érvényes Aláírás létrehozó adat.

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

4.6. Biztonsági audit eljárások

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

4.6.1. Naplózott esemény típusok

A Szolgáltató hitelesítés támogató informatikai rendszerén az 5.2.2 pontban meghatározott szerepkörű munkatársai által végzett műveletek naplózásra kerülnek, amelyeket a regisztráció, a tanúsítvány igénylés, tanúsítvány visszavonás, tanúsítvány állapot közzététel, az Aláírás létrehozó és ellenőrző adatpár generálása, az Aláírás létrehozó eszköz megszemélyesítése, a Tanúsítvány létrehozása és kibocsátása, valamint az időbélyegzés során hajtanak végre.

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 minősített tanúsítvány aláíró, infrastruktúrális és kontroll kulcs tanúsítványainak életciklusával kapcsolatos összes eseményt ezen belül különösen:
  - a Tanúsítvány előállítási és megújítási igények benyújtásának időpontját,
  - az igények teljesítésének időpontját.

Az aláírók Aláírás létrehozó eszközzel való ellátásával kapcsolatosan[35]:

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

A visszavonás kezeléssel kapcsolatosan a Szolgáltató gondoskodik a felfüggesztéssel/visszavonással kapcsolatos összes kérés, valamint az ezek következtében előállt tevékenység naplózásáról

Az időbélyegzéssel kapcsolatosan:

- az időbélyegzés szolgáltatás fő lépései, a kérelemtől az időbélyeg válasz elküldésig,
- az időbélyeg aláíró kulcs életciklusában bekövetkező események (generálás, használat, visszavonás, megsemmisítés),
- az időbélyeg aláíró kulcs tanúsítványa életciklusában bekövetkező események (kiadás, használat, visszavonás).

A hitelesítés-szolgáltatást támogató informatikai rendszer biztonságával kapcsolatosan:

- a napló adatok integritásának megsértésével,
- a naplózási funkció elindításával és leállításával,
- a naplózási paraméterek megváltoztatásával,
- a naplózás tárolásával kapcsolatos hibákkal,
- a hitelesítés-szolgáltatást támogató informatikai rendszerhez történő bármely hozzáférési kísérlettel

kapcsolatos eseményeket rögzíteni kell.

A naplózott adatállománynak tartalmaznia kell a naplózott esemény bekövetkeztének dátumát és pontos idejét, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az esemény kiváltásában közreműködő felhasználó vagy más személy nevét vagy azonosítóját.

A pontos időt a Szolgáltató pontos idő egysége biztosítja, ami legfeljebb 1 másodperces eltérést engedélyez a valódi időhöz képest. Az esetleges ennél nagyobb eltérések szintén naplózásra kerülnek.

[35] Az „Aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése” szolgáltatás keretén belül.

A hitelesítés szolgáltatást támogató informatikai rendszer operációs rendszerére, illetve a rendszer többi elemeire vonatkozóan a Biztonság politikában és a Biztonsági Szabályzatban meghatározott események kerülnek naplózásra.

4.6.2. Napló adatok feldolgozásának gyakorisága

A nyilvános kulcsú hitelesítés (PKI), az időbélyegzés alkalmazás és az operációs rendszer szintű biztonsági esemény és audit naplók operatív (napi) ellenőrzését csak a rendszer vizsgálók (auditorok) végezhetik csak olvasási jogosultsággal. A rendszer vizsgálók feladata a PKI alkalmazáson és operációs rendszeren kívüli, de a Trust&Sign Rendszer részét képző szoftver elemek (hálózat, tűzfalak, betörés detektor) naplóinak ellenőrzése is.

A rendszer auditorok a Szolgáltató informatikai biztonsági menedzserének jelentik a rendellenességeket, aki félévente rendszeres belső auditot, illetve szúrópróbaszerű eseti ellenőrzéseket végez.

4.6.3. Napló adatok tárolási ideje

A 16/2001. (IX. 1.) MeHVM rendelettel összhangban az archivált naplókat keletkezésüktől számított 10 évig, illetőleg a velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig megőrződnek[36] meg kell őrizni. Papír alapú naplókat csak abban az esetben kell megőrizni, ha nincs elektronikus megfelelőjük.

4.6.4. Napló adatok védelme

A hitelesítés és időbélyegzés szolgáltatás támogató informatikai rendszer biztonsági szempontból legkritikusabb elemei – így a naplóik is –, fokozott biztonságú fizikai környezetben vannak. A naplók elektronikus aláírással hitelesítettek és hozzáférési jogosultsággal nem rendelkezők által nem olvashatók. A környezeti, kulcsgondozási és a tanúsítványkezelési események időbélyegzővel ellátva kerülnek naplózásra.
A biztonsági és esemény naplókhoz csak a rendszer auditor, az informatikai biztonsági adminisztrátor, valamint a külső auditor férhetnek hozzá, csak olvasási joggal.

[36] A 2001. évi XXXV. törvény 9. § (7)

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

A Szolgáltató biztosítja a tanúsítványok, időbélyegek és kulcsok gondozására vonatkozó napló rekordok bizalmasságát és sértetlenségét.

4.6.5. Napló adatok mentési eljárásai

A hitelesítés és időbélyegzés szolgáltatás támogató informatikai rendszer különböző moduljaiban elkészült naplók egy központi mentő szerveren kerülnek összegyűjtésre. A mentő szerver és az egyedi eszközök tartalmának mentése hetente egyszer rendszeresen megtörténik egyszer írható médiára rejtjelezett és elektronikusan aláírt formában. Az ily módon mentett napló állományok visszaállíthatók az eredeti formájukba. A mentés és visszaállítás operatív folyamatait a Szolgáltató Üzemeltetési Szabályzata írja le részletesen.

A mentések első, másod és harmad példányai megőrzésre kerülnek.

4.6.6. A naplók gyűjtési rendszere

A naplók és a mentést tartalmazó adathordozók a Szolgáltató Bizalmi központjának technikai helyiségében elhelyezett páncélszekrényben, a napló mentés biztonsági példánya a Biztonsági Adattárban elhelyezett páncélszekrényben, a harmadik példány a katasztrófa helyszínen kerül elhelyezésre.

4.6.7. Rendkívüli eseményekről történő értesítés

A szolgáltatás támogató informatikai rendszerre, annak fizikai és személyi környezetére kihatható súlyos üzemzavari és katasztrófa események megelőzéséről, kezeléséről, az érintettek értesítéséről és a rendszer visszaállításáról részletesen az Üzletmenet-folytonossági Terv intézkedik, a lényeges intézkedéseket a 4.9. fejezet tartalmazza.

Az üzletmenet-folytonosságot veszélyeztető, sértő, illetve megszüntető események az Üzletmenet-folytonossági Tervben súlyossági osztályokba vannak sorolva. Ez a Terv a szokásos üzletmenet-folytonossági tervekhez képest annyiban különbözik, hogy részletesen szabályozza az 1. és a 2. szintű Hitelesítő Központok saját Aláírás létrehozó adatainak, aktiváló adatai-

nak (PIN kódok, jelszavak) és az időbélyegek aláíró kulcsának kompromittálódása esetén elvégzendő teendőket.

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.

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

4.6.8. Sebezhetőség kiértékelése

A hitelesítés szolgáltatás támogató informatikai rendszernek és annak fizikai és személyi környezetének a biztonsági sebezhetőségét két szempontból kell mérni:

- Az informatikai rendszer által kezelt adatok bizalmasságának, hitelességének és sértetlenségének (röviden: az információvédelem) sérülése vagy elvesztése, ebbe beletartozik a Szolgáltató saját Aláírás létrehozó adatainak és aktiváló adatainak kompromittálódás elleni védelme is,
- Az informatikai rendszer által kezelt adatok rendelkezésre állásának sérülése vagy elvesztése, amelynek kritikus mértékét az Üzletmenet-folytonossági Tervben meghatározott sebezhetőségi rés (a szolgáltatások kiesésének elviselhető mértéke egy hónapra vetítve, 7*24 órás folyamatos üzemet feltételezve).

A sebezhetőséghez kapcsolódó kockázatok a szolgáltató rendszerének megvalósítása előtt becsült kockázatok, és a megvalósítás utáni (maradék) kockázatok elemzése és értékelése megtörtént és a szükséges védelmi intézkedések végrehajtásra kerültek.

Az aktuális sebezhetőségi szintek a biztonsági ellenőrzése és kiértékelése a 6.5.2 pont 3. táblázata szerinti rendszerben történik.

4.7. Adatarchiválás

A Szolgáltató gondoskodik arról, hogy a tanúsítványokra és az időbélyegzésre vonatkozó minden lényeges információ megfelelő ideig rögzítésre kerüljön, különösen jogi eljárásokhoz bizonyíték nyújtása érdekében.

4.7.1. 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 Központ és/vagy a küldő regisztrációs felügyelő (RO) azonosítója, amennyiben ez értelmezhető.
- A 4.6.1 pontban felsorolt összes esemény, illetve napló típus.

Azon eseményeket, mely a fent említett naplóbejegyzéseken túl kerülnek archiválásra (a biztonságos környezet fenntartásának és utólagos ellenőrizhetősége és bizonyíthatósága céljából), a HSzSz 5.1 pontja határozza meg.

4.7.2. Az archívum megőrzési időtartama

A Szolgáltató 4.7.1 pontban megnevezett nyilvántartásokat és naplókat a 16/2001. (IX.1.) MeHVM rendelettel összhangban a keletkezésüktől számított 10 évig, illetve jogi eljárásban a tanúsítványokon keresztül történő bizonyításhoz szükséges ideig megőrzi.

4.7.3. Az archívum védelme

A Szolgáltató az archívumában és a Biztonsági Adattárában olyan fizikai védelmet biztosít, amely fenntartja a tanúsítványokra és az időbélyegzésre vonatkozó aktuális és archivált adatok bizalmasságát és sértetlenségét

Az archívumba és a Biztonsági Adattárba történő belépéshez csak az Szolgáltató informatikai biztonsági menedzsere és a rendszer auditor rendelkezik jogosultsággal.

Az archívumba és a Biztonsági Adattárba történő adattovábbítás csak bizalmasság sérülése elleni védelemmel ellátva, elektronikusan aláírva és időbélyegzéssel ellátva történhet.

Az archívumba és a Biztonsági Adattárba érkező iratokat és adathordozókat az érkezési időpontot is tartalmazó nyilvántartásba kell venni, amellyel követni kell az előforduló irat és adathordozó mozgásokat (kivétel, visszaadás, megsemmisítés).

A Szolgáltató megfelelő műszaki és szervezeti védelmi intézkedéseket hoz, amelyek megvédik a személyes adatokat a felhatalmazás nélküli, illetve törvénytelen feldolgozás ellen, valamint a személyes adatok véletlen elveszése, megsemmisülése, illetve károsodása ellen.

4.7.4. Az archívum mentési folyamatai

A Szolgáltató a tanúsítványokra és az időbélyegzésre vonatkozó naplóadatokat teljes körűen és a bizalmasságot garantáló módon archiválja.

4.7.5. A rekordok időbélyegzésére vonatkozó követelmények

Az archivált adatállományok időbélyegzővel ellátottak.

4.7.6. Az archívum gyűjtési rendszere

Az archivált adathordozók első példányai a Szolgáltató archívumában, a biztonsági példányai a Biztonsági Adattárban, a harmadik példányok a katasztrófa helyszínen kerülnek elhelyezésre.

4.7.7. Archív információ hozzáférését és ellenőrzését végző eljárások

A Szolgáltató az archívumhoz Ügyfélkapcsolati Irodáján 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.

4.8. Kulcs csere

A Szolgáltató által kibocsátott előfizetői tanúsítványok érvényességi ideje 1 év. Az érvényesség kezdete a kibocsátás ideje. Az Aláírás létrehozó adatok érvényességi ideje megegyezik a Tanúsítvány érvényességi idejével. A Szolgáltató lehetőséget biztosít az előfizetők részére a Tanúsítvány lejártát megelőző 30 napos időszakban arra, hogy a Tanúsítványt megújítsák, a hozzá tartozó kulcspár cseréje mellett.

Előfizetői tanúsítvány egy alkalommal frissíthető, egy éves időtartamra. A frissítés igénylése a 3.2 pontban leírtak szerint történhet. A második frissítési kérelemnél az Aláírónak új Tanúsítványt kell igényelnie a kezdeti regisztráló eljárás módszerével és új kulcspár előállítása mellett. A kulcspár generálást a Trust&Sign® szolgáltatások esetében mindig a Szolgáltató végzi.

A megújított Tanúsítvány érvényességének kezdete a megújítás időpontja lesz.

A Szolgáltatói Aláírás létrehozó adatok megújítására előre tervezetten abban az esetben kerül sor, ha a kulcs érvényessége lejár, és azt nem hosszabbítják meg. Ebben az esetben a Szolgáltató a lejáratot megelőzően intézkedik az új, a szolgáltatói Aláírás létrehozó adat létrehozásának szabályai szerint történő előállításra és annak elkészültét valamint digitális lenyomatának publikálását követően, az előfizetők igénye alapján megkezdi részükre az új magánkulccsal aláírt tanúsítványok kiadását. A nem tervezett kulcs változtatás esetei a 4.9 pontban találhatók.

4.9. Katasztrófa elhárítás, Aláírás létrehozó adat kompromittálódás

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.

A Szolgáltató Üzletmenet-folytonossági Tervében a katasztrófa események az üzletment-folytonosságot sértő események legszigorúbb osztályát képezik, így katasztrófa megelőzési és elhárítási intézkedések a Terv szerves részét képezik.
A következő pontokban szereplő esetekre az Üzletmenet-folytonossági Terv részletes intézkedéseket tartalmaz.

4.9.1. Hardver, szoftver, vagy adatsérülés esete

A hardver, illetve szoftver meghibásodások, üzemzavarok osztálybasorolástól függő intézkedéseket vonnak maguk után. Katasztrófa esetben az Üzletmenet-folytonossági Tervben előírt azonnali reakciós intézkedéseket kell foganatosítani, azaz értesíteni kell:

- a Szolgáltató meghatározott felső vezetőit,
- a Válság Stáb vezetőjét és tagjait,
- szükség esetén a szerződéssel lekötött szerviz cégeknek, az Üzletmenet-folytonossági Tervben megnevezett munkatársai.

A Válság Stáb első intézkedései:

- a katasztrófa esemény azonosítása és behatárolása,
- A katasztrófa esemény további hatásainak korlátozása,
- A károk azonosítása, a további károk keletkezésének megakadályozása, illetve mérséklése és a kárérték becslése.

A Válság Stáb további intézkedései a hitelesítés szolgáltatást támogató informatikai rendszer részleges vagy teljes visszaállítására vonatkoznak a katasztrófa tartalék helyszínen**.**

A visszaállítás egyik alapfeltétele a megfelelő program és adatmentések rendelkezésre állása. A Szolgáltató Üzemeltetési Kézikönyve részletesen tartalmazza a hitelesítés szolgáltatást és időbélyegzést támogató informatikai rendszere egyes részrendszereire:

- a teljes rendszer mentés gyakoriságát és időpontját,
- az inkrementális mentések gyakoriságát és időpontját,
- a program, file, könyvtár, tranzakció mentések gyakoriságát és időpontját
- a szükséges adathordozó típust és kapacitást.

Minden mentés három példányban készül. Az első példány a Szolgáltató archívumában, a második, biztonsági példány a Biztonsági Adattárban, a harmadik példányok a katasztrófa helyszínen kerülnek tárolásra. A mentések bizalmasság sérülés elleni védelemmel ellátva, időponttal ellátva és elektronikusan aláírva kerülnek tárolásra.

4.9.2. 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 a 2.6.1 pont szerint,
- 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 – amennyiben az sérült –, valamint a végfelhasználók számára új nyilvános kulcsot biztosít új Tanúsítvány kiadásával.

4.9.3. Egy szolgáltatói egység kulcsának kompromittálódása

Egy szolgáltatói kulcs kompromittálódása esetén a Szolgáltató az alábbiakat vállalja:

- a kompromittálódásról tájékoztatja az összes előfizetőt és érintett felet a 2.6.1 pont szerint,
- jelzi, hogy az adott szolgáltatói kulcs felhasználásával kiadott tanúsítványok, időbélyegek és visszavonási állapot információ már nem érvényes(ek).

A Szolgáltató a szolgáltatói kulcs kompromittálódását előidéző okok megszüntetése érdekében helyreállítja a biztonságos környezetet, valamint szükség esetén új kulccsal és tanúsítvánnyal látja el a szolgáltatói egységet, valamint a kompromittálódás által érintett végfelhasználókat.

Katasztrófa esemény osztályba sorolt az Elsődleges Hitelesítő Központ („Root”), illetve a Szolgáltató operatív hitelesítő Aláírás létrehozó adatainak, az időbélyeg aláíró kulcsnak, az aktiváló adatoknak és a hardver biztonsági moduloknak az együttes kompromittálódása. Az Üzletmenet-folytonossági Terv forgatókönyvet tartalmaz az ilyen típusú katasztrófa eseményre.

Ez a szolgáltatás azonnali felfüggesztésével jár és amennyiben a kompromittálódás ténye bizonyítást nyer, az összes tanúsítványt vissza kell vonni, és az időbélyeg kibocsátást le kell tiltani. A szolgáltatások felfüggesztésének tényéről a Szolgáltató értesíti a Szolgáltató és a felhasználó Közösség tagjait, valamint a Hírközlési Felügyeletet.

4.9.4. 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 az Üzletmenet-folytonossági Tervben megjelölt időn belül.

A visszaállítási időt alapvetően az esemény súlyossága, azaz az Üzletmenet-folytonossági Terv szerint értelmezett osztályba sorolása határozza meg. A súlyos üzemzavari és a katasztrófa esetet – többek között – az különbözteti meg, hogy katasztrófa esetén nagy valószínűséggel nem csak az informatikai rendszer, hanem annak a fizikai környezet is megsemmisül részben vagy egészben. Ez utóbbi esetben az Üzletmenet-folytonossági Tervben meghatározott módon a Válság Stáb intézkedik a katasztrófa tartalékhelyre történő áttelepülésről és az informatikai rendszer részleges vagy teljes visszaállításáról a katasztrófa helyszínen korábban elhelyezett mentések segítségével.

Ilyen esetekben szolgáltató a következő szolgáltatások legfeljebb 3 órán belüli elindítását vállalja:

- visszavonás kezelés szolgáltatás,
- visszavonási állapot közzététele szolgáltatás.

Minden egyéb szolgáltatás elindítását szolgáltató 24 órán belül vállalja.

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

4.9.5. Üzletmenet-folytonossági Terv

A Szolgáltató rendelkezik Üzletmenet-folytonossági Tervvel, amely részletes intézkedési forgatókönyveket tartalmaz a különböző osztályú üzemzavari, illetve katasztrófa események kezelésére. Ez a dokumentum biztonsági okokból nem nyilvános.

4.10. 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 visszavonás kezelés és közzététel szolgáltatások fenntartásáról.

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

- tájékoztatja az összes Előfizetőt és Érintett felet[37] a 2.6.1 pont szerint;

  a Szolgáltató a szolgáltatások megszűnése esetén késlekedés nélkül értesíti a Szolgáltató és a felhasználó Közösség tagjait és a Hírközlési Felügyeletet. Amennyiben a megszűnés tervezett, az értesítés legkevesebb 60 nappal megelőzi a szolgáltatás leállítását.

- megszűnteti 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 4.7) fenntartására vonatkozó kötelezettségeket átruházza arra az időtartamra, amelyről az előfizetőket és az érintett feleket tájékoztatta (lásd 2.6),

- letiltja az időbélyegek kibocsátását,

- magánkulcsait megsemmisíti, illetve visszavonja a használatból a 6.2.9 alatt meghatározottak szerint.

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

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.

A Szolgáltató a tervezett megszűnés előtt tárgyalásokat kezd más szolgáltatókkal a szolgáltatások átvételéről. A tárgyalások végeredményéről tájékoztatja a közösséget. Az értesítést a szolgáltatások nyújtásában részt vevő szervezeteknek és az előfizetőknek elektronikus aláírásával ellátott e-mailben küldi el, s az érintett felek tájékoztatása végett a web oldalain és két országos napilapban is közzé teszi.

A bejelentéssel egyidejűleg a Szolgáltató leállítja:

- tanúsítvány előállítás szolgáltatást (ezen belül a Tanúsítvány megújítását),
- az időbélyegzés szolgáltatást,
- kezdeti regisztráló szolgáltatást (egyéb regisztráló szolgáltatások tovább élnek),
- tanúsítvány kibocsátás szolgáltatást (ezen belül a tanúsítványok archiválását),
- Biztonságos aláírás-létrehozó eszközön az Aláírás-létrehozó adat elhelyezése szolgáltatást.

Szolgáltató a tervezett megszűnés előtt 20 nappal intézkedik az előfizetői tanúsítványok és saját felhasználású tanúsítványok visszavonásáról.

Ezzel egyidejűleg leállítja a visszavonás kezelési szolgáltatást.

Szolgáltató nem biztosít a szokásosnál és a jogszabályokban előírtnál nagyobb mértékű adatszolgáltatást a megszűnéskor.

Eljárás Regisztrációs Iroda megszűnése esetén:

- A Regisztrációs Iroda megszűnése előtt 60 nappal értesíti azon előfizetőket, akik a megszűnő Regisztrációs Irodától kapott, a Szolgáltató által kibocsátott érvényes tanúsítvánnyal rendelkeznek.
- A Regisztrációs Iroda megszűnéséről a felhasználó Közösség tagjait Szolgáltató a web oldalain történő közzététel útján tájékoztatja.

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 és időbélyegzéssel 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 szabályzat 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[38].
- A Szolgáltató a Biztonsági Szabályzatában dokumentálta, majd megvalósította és folyamatosan fenntartja a hitelesítési és időbélyegzési szolgáltatásokat nyújtó eszközök, rendszerek és informatikai értékek biztonsági ellenőrzéseit és üzemeltetési eljárásait.
- A Szolgáltató gondoskodik az informatika biztonság fenntartásáról azokban az esetekben is, amikor az elektronikus aláírással és időbélyegzéssel 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

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

- 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 személyzet hajthatja végre.

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

A Szolgáltató fizikai, az eljárásrendi (adminisztratív) és a humán biztonsági szabályozásokat a Biztonsági Szabályzat tartalmazza részletesen. A Biztonsági Szabályzat biztonsági okokból nem nyilvános.

A szolgáltatás támogató informatikai rendszer és annak személyi, valamint fizikai környezete a MeH 12. ajánlás szerint lett fokozott biztonsági osztályba sorolva, amely egyértelműen meghatározza az Elsődleges Hitelesítő Központ, a másodlagos hitelesítő központok, az időbélyegző központ és a regisztrációs irodák informatikai rendszereinek, személyi és fizikai környezetének biztonsági követelményeket.

A következő pontok csak a vonatkozó lényeges intézkedéseket tartalmazzák.

5.1. Fizikai biztonsági szabályozások

5.1.1. Hitelesítő Központok

Ebben a pontban az Elsődleges Hitelesítő Központon kívül a fizikai objektumokban létező (nem logikai) másodlagos hitelesítő és időbélyegző központok fizikai biztonsági szabályairól lesz szó.

A hitelesítő és időbélyegző központok legmagasabb védelmi szintet képező objektuma a Bizalmi Központ, amely a biztonsági szempontból legkritikusabb hardver/szoftver modulokat tartalmazza. Ez az objektum fokozott biztonsági osztályba sorolt, amely a következő, a MeH 12. ajánlás szerinti főbb fizikai védelmi követelményeknek felel meg:

- a fokozott biztonsági szintnek megfelelő szilárdságú határoló felületek,
- a Bizalmi Központ bejárati ajtaja és a technikai helyiség ajtaja a MABISZ ajánlásában meghatározott I-es kategóriájú, a perszonalizációs helyiség ajtaja MABISZ III. kategóriájú,
- a Bizalmi Központ objektum előtt biztonsági szegmens van kialakítva, amelybe anti-passback és naplózási tulajdonságokkal bíró beléptető rendszere keresztül lehet csak bejutni,
- a Bizalmi Központba történő bejutást video biztonsági kamerás rendszer figyeli, amelynek személyes felügyelete folyamatosan biztosított,
- a Bizalmi Központ rendelkezik önálló és kettőzött klimatizálással, valamint mozgásérzékelő, tűz- és füstjelző és tűzoltó rendszerrel,
- a Bizalmi Központ IT eszközei két, egymástól független külső betáplálással támogatott, Diesel aggregátoros, szünetmentes tápáramellátó rendszerrel rendelkezik,
- a Bizalmi Központban a szerverek biztonsági kabinetekben vannak elhelyezve,
- a Bizalmi Központra és a kabinetekre a Biztonsági Szabályzat egy fejezetét képező kulcskezelés szabályozás érvényes,
- a Bizalmi Központ az MSZ 274/5T:1993 szabvánnyal összhangban LPZ2 zónahatárig kiépített másodlagos villámvédelemmel ellátott,
- a Bizalmi Központba csak a Biztonsági Szabályzatban meghatározott szerepkörű vezetők és munkatársak léphetnek be,
- a mentési és a primer szoftver adathordozók, a nyers és a megszemélyesített Aláírás létrehozó eszközök besugárzás és fizikai behatás ellenálló biztonsági szekrényekben tároltak,
- a működtetési és menedzselési és a biztonsági dokumentáció elektronikusan tárolt,
- a Szolgáltató az érzékeny adatokat tartalmazó adathordozó eszköztől biztonságosan válik meg, amennyiben azokra már nincs szükség,
- 60 DB elnyomással rendelkező EMC védelemmel ellátott,

- az informatikai rendszer két független nyomvonalon vezetett üvegkábellel kapcsolódik az Internethez,
- a lokális telefonkapcsolat az EMC zónahatáron szűrőn keresztül kapcsolódik a szolgáltató telefonközpontjához.

A környezetei elemek, rendszerek alábbi állapotjellemzőit monitor rendszer figyeli:

- hőmérséklet,
- páratartalom
- légnyomás,
- tűzeset érzékelés,
- tápáramellátás üzemkészség,
- légkondicionáló rendszer üzemkészség,
- biztonsági rendszer jelzései.

A bekövetkező események naplózásra, majd archiválásra kerülnek.

5.1.2. Regisztrációs Iroda

A regisztrációs tevékenység a Bizalmi Központ perszonalizációs helyiségében folyik, amely az előző pontban ismertetett fokozott biztonságú fizikai védelemmel van ellátva. Itt találhatók a regisztrációs munkahelyek és munkaállomások.

5.2. Eljárásrendi szabályozások

A Szolgáltató Eljárásrendi Szabályait három szabályzat tartalmazza:

- a Szervezeti és Működési Szabályzat, amely részletesen meghatározza a Szolgáltató szervezeti felépítését, azon belül az egyes munkaköröket és az azokhoz kapcsolt feladat-, felelősség és hatásköröket,
- a jelen HSzSz,
- a Biztonsági Szabályzat, amely részletese szabályozza az adatokhoz, az informatikai rendszerhez, a személyi és a fizikai környezethez kapcsolódó biztonsági szabályokat.

5.2.1. Bizalmi munkakörök

Jelen pont 2. táblázatában a hitelesítés és időbélyegzés szolgáltatáshoz kapcsolódó szerepköröket, azok feladat-, felelősség és hatáskörei kerülnek összefoglalásra.

Szerepkör	Feladatkör	Felelősségi kör	Hatáskör
A Szolgáltató vezetője	A Szolgáltató szervezet irányítása és ellenőrzése	Folyamatos és biztonságos szolgáltatás. A Trust&Sign Rendszer és adat tulajdonosa	A Szolgáltató munkáltatói jogköre. A teljes szervezet szintjén dönt
A PKI Üzleti Egység vezetője	A Szolgáltató szervezet szolgáltatási tevékenységének irányítása és ellenőrzése	Folyamatos és biztonságos szolgáltatás. Trust&Sign Rendszer működtetésének egyszemélyi felelős vezetője	A Szolgáltató szervezet szintjén dönt, intézkedik.
Ügyfélkapcsolati Iroda vezető	Az ügyfélkapcsolati tevékenység irányítása és ellenőrzése.	Az ügyfelek biztonságos azonosítása-hitelesítésének ellenőrzése.	Az ügyfélkapcsolati tevékenység ellenőrzése.
Hitelesítés Pol. és Szab. Csop. Vezető	Politikák, szabályzatok kialakítása, PKI belső ellenőrzés	Politikák, szabályzatok és gyakorlat összhangja	Politikák, szabályzatok érvényesítése, PKI belső audit
A Szolgáltató IB vezetője	IB tevékenység irányítása, ellenőrzése a Szolgáltató minden területén.	IB kockázatok elviselhető szinten tartása	IB intézkedések, IB belső ellenőrzés.
Üzemeltetés vezető	Az IT rendszer üzemeltetés irányítása	Az üzemeltetés folyamatossága, minősége, biztonsága	Intézkedés az IT rendszer minden szintjén üzemeltetési kérdésekben
Üzemeltető adminisztrátor	Üzemeltetési adminisztráció, hibaelhárítás, karbantartás	Az üzemeltetés folyamatossága, minősége	Operatív intézkedés az üzemeltetés területén
IB adminisztrátor	Biztonsági beállítások, adminisztráció, karbantartás	Az üzemeltetés biztonsága	Operatív ellen-őrzés, operatív intézkedés
Hitelesítő biztonsági felügyelő (Security Officer /SO/)	RO kulcsok, tanúsítványok létrehozása	Saját kulcs, PKI és időbélyegzés alkalmazás és adatok biztonsága	RO és ügyfél kulcsok, tanúsítványok létrehozása. RO hatásköre is lehet.
Regisztrációs felügyelő (Registration Officer /RO/)	Regisztrációs Iroda irányítás. Előfizető regisztráció, kulcs, ta-	Regisztrációs Iroda folyamatos működtetése.	Regisztrációs Irodán intézkedési jog. SO hatásköre nem lehet.

Szerepkör	Feladatkör	Felelősségi kör	Hatáskör
	núsítvány igénylés, kulcs megszemélyesítés		
Rendszer operátor	Üzemeltetési rutin tevékenységek PKI szinten.	A PKI és időbélyegzés alkalmazás üzemeltetésének folyamatossága,	Rutin operátori tevékenység az Üzemeltetési Kézikönyv szerint
Rendszer vizsgáló (auditor)	Operatív funkcionális és biztonsági ellenőrzések.	Funkcionális és biztonsági hiányosságok, visszaélések felfedése.	Biztonsági és audit naplók ellenőrzése.

2. táblázat

5.2.2. Az egyes feladatokhoz szükséges személyzeti létszámok

Általánosan teljesül a Szolgáltató egészére, hogy minden munkatárs csak a saját munkakörének megfelelő funkciókat aktivizálja[39].

A Szolgáltató Bizalmi Központjában a bizalmi szerepköröket betöltő munkatársak a következő feladatokat végzik el:

Két SO együttes jelenléte (és előzetes, sikeres hitelesítése) szükséges az alábbi funkciók kiváltásához:

- a Szolgáltató első saját kulcsának generálása a Szolgáltató vezetője által kijelölt bizottság jelenlétében (lásd 6.1.1),
- a Szolgáltató későbbi saját kulcsainak generálása a Szolgáltató vezetője által kijelölt bizottság jelenlétében (lásd 6.1.1),
- a Szolgáltató magán aláíró kulcsainak biztonsági mentése (lásd 6.2.4)
- a Szolgáltató magán aláíró kulcsainak (teljesítmény növelés céljából végrehajtott) másolásánál (klónozása) (6.2.6),
- a Szolgáltató magán aláíró kulcsainak visszaállítása (lásd 6.2.2)
- a Szolgáltató magán aláíró kulcsainak (és annak összes másodpéldányának) megsemmisítése (lásd 6.2.9),

[39] Az egyes munkakörök egymástól elválasztva, külön-külön működnek. Tilos más munkatárs részére hozzáférési jog átengedése (a birtokolt intelligens kártya és a hozzá tartozó jelszó átadásával, vagy egy már érvényesen hitelesített, megnyitott munkafolyamat folytatásának lehetővé tételével).

- a Szolgáltató nyilvános kulcsait tartalmazó token Root CA-hoz való továbbításánál, illetve az erre, a Root CA által kibocsátott Tanúsítvány visszaszállításánál a Szolgáltató vezetője által kijelölt bizottság jelenlétében (lásd 6.1.3),
- a Root CA nyilvános kulcsát tartalmazó tokennek a Produktív CA-hoz való továbbításánál a Szolgáltató vezetője által kijelölt bizottság jelenlétében (lásd. 6.1.4),
- az RO kulcsok[40] kezdeti generálása, cseréje és megsemmisítése.

Az SO feladatai a fentieken kívül a következők:

- a PKI és időbélyegző alkalmazói szoftverek integritásának biztosítása és ellenőrzése,
- a biztonsági és audit naplók beállítása PKI és időbélyegző alkalmazás szinten a naplózási és audit politikának (HSzSz 4.6) megfelelően,
- a PKI alkalmazások üzemszerű leállítása (a szolgáltatások nem csorbulnak, tanúsítvány visszavonást nem von maga után),
- a PKI és időbélyegző alkalmazások vész-leállítása katasztrófa esemény, Root CA privát kulcs, CA privát kulcs kompromittálódás, vagy egyéb komoly üzemzavar esetén, amikor a katasztrófa tartalék megoldás lép életbe (HSzSz 4.9),
- felmerülő probléma esetén hibakeresés és javítás PKI és az időbélyegző alkalmazások szinten,
- rendszeres archiválás nem újraírható adathordozóra (CD-R).

Az SO-knak a Szolgáltató Biztonsági Szabályzatában meghatározott módon jelentési kötelezettségük van a PKI Üzleti Egység vezetője és a Szolgáltató informatikai biztonsági vezetője felé.

Az RO-k feladatai a következők:

- jóváhagyja a tanúsítványok előállítását, visszavonását és felfüggesztését, pontosabban ennek az Ügyfélkapcsolati Irodánál keletkező és a Regisztrációs Iroda felé irányuló kérését,
- ellenőrzi az Ügyfélkapcsolati Iroda által felvett ügyfél adatokat és az ügyfél azonosítás-hitelesítés eredményességét,
- kulcspárokat generál(tat) az aláírók számára (lásd 6.1.1),
- elvégzik a Biztonságos aláírás-létrehozó eszközök megszemélyesítését,

[40] Melyek a Regisztrációs Iroda biztonságos (hiteles és bizalmas) kapcsolatát teszik lehetővé a Hitelesítő Központtal.

- biztonságos módon megsemmisíti az Aláíró részére előállított magánkulcs Biztonságos aláírás-létrehozó eszközön kívüli összes példányát, miután az Aláíró részére előállított kulcspárt elhelyezte az Aláírás létrehozó eszközön,
- aktivizálják a Biztonságos aláírás-létrehozó eszközöket aktivizáló PIN kódok generálását, kinyomtatását és borítékolását végrehajtó funkciókat (lásd 6.4.1),
- ellenőrzik a Biztonságos aláírás-létrehozó eszközök kiiktatását, megsemmisítését, illetve újraaktivizálását (lásd 6.1.2),
- gondoskodnak a Biztonságos aláírás-létrehozó eszközök biztonságos tárolásáról (a címzettekhez történő továbbításig) (lásd 6.1.2),
- biztosítja saját Aláírás létrehozó adatainak biztonságos használatát és tárolását,
- intézkedik saját Tanúsítványának visszavonása, illetve felfüggesztése végett, amennyiben magánkulcsa kompromittálódott, vagy ennek gyanúja áll fenn,
- fogadja a Hitelesítő Központtól kapott új tanúsítványokat, valamint ellenőrzi ezek hitelességét és sértetlenségét,
- kezdeményezi az új tanúsítványok elküldését a Címtárnak, biztosítva az ezt tartalmazó üzenet hitelességét és sértetlenségét,
- kezdeményezi az új Tanúsítvány visszavonási lista elküldését, biztosítva az ezt tartalmazó üzenet hitelességét és sértetlenségét,
- az Előfizető és az Aláíró minden személyes adatát, – kivéve a Tanúsítványba kerülőket – a személyes adatok védelméről szóló 1992 évi LXIII. törvénynek megfelelően kezeli, s csak a HSzSz 2.8.3 - 2.8.7 pontokban említett esetekben és személyek részére fedi fel őket,
- 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,
- visszautasítja (az ok megjelölésével) a nem hiteles, érvénytelen, vagy szabálytalan, tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket.

Az RO-knak a Szolgáltató Biztonsági Szabályzatában meghatározott módon jelentési kötelezettségük van a PKI Üzleti Egység vezetője és a Szolgáltató informatikai biztonsági vezetője felé.

Az infrastruktúra szintű IB adminisztrátorok hajtják végre a következő feladatokat:

- a központi és regisztrációs biztonsági tisztviselők, illetve a (mindkét típusú) rendszeradminisztrátorok rendszerhez való hozzáférésének kezelése, mely magában foglalja az alábbiakat:
  - rendszer-felhasználók felvétele,
  - felhasználói jogosultságok beállítása,
  - kezdeti jelszó meghatározása,
  - a távozó, illetve munkakört váltó rendszer-adminisztrátorok hozzáférési jogainak azonnali megszüntetése,

A rendszervizsgáló feladatai a következők:

- ellenőrzi és archiválja a Bizalmi Központ technikai helyiségében működő PKI és időbélyegző alkalmazások biztonsági naplóit,
- ellenőrzi és archiválja a Bizalmi Központ technikai helyiségében működő PKI és időbélyegző szerverek operációs rendszer szintű naplóit,
- ellenőrzi és archiválja a Bizalmi Központ technikai helyiségében működő tűzfalak és az betörés detektor biztonsági naplóit,
- ellenőrzi és archiválja a Bizalmi Központ technikai helyiségében működő web szerver és LDAP szerverek biztonsági naplóit.

A rendszervizsgálóknak a Szolgáltató Biztonsági Szabályzatában meghatározott módon jelentési kötelezettségük van a PKI Üzleti Egység vezetője és a Szolgáltató informatikai biztonsági vezetője felé.

A rendszervizsgáló a fenti feladatok mellett, szükség esetén az általa készített archívumokban keresést végez. A Szolgáltató (ideiglenes és állandó) munkatársainak részletes munkaköri leírásai támogatják a feladatok szétválasztása és a legkisebb meghatalmazás szempontjait. A munkaleírások többek között meghatározzák az egyes feladatokhoz szükséges létszámot is.

5.2.3. Az egyes munkakörökben elvárt azonosítás és hitelesítés

A Hitelesítő Központnál az SO-k, RO-k azonosítása és hitelesítése egy intelligens kártyaolvasóba helyezésével, majd az azt aktivizáló PIN kód megadásával történik.

Sikeres hitelesítés előtt egyetlen biztonság kritikus tevékenységet sem lehet végrehajtani.

A Regisztrációs Iroda valamennyi bizalmi munkakört betöltő munkatársának azonosítása és hitelesítése egy intelligens kártyaolvasóba helyezésével, majd az azt aktivizáló PIN kód megadásával történik.

Sikeres hitelesítés előtt egyetlen biztonság kritikus tevékenységet sem lehet végrehajtani.

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 és az időbélyegzéssel 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 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 és az időbélyegzési 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 2. táblázatban meghatározott szerepkörök mindegyikéhez történő személy hozzárendelésnél az átlagosnál magasabb szint biztonsági ellenőrzés történik. Közülük a következők minősülnek olyan szerepkörnek, amely biztonsági ellenőrzésre feljogosít:

- A PKI Üzleti Egység vezetője
- Hitelesítés Pol. és Szab. Csop. Vez.
- Ügyfélkapcsolati Iroda vezető
- A Szolgáltató IB vezetője
- IB adminisztrátor
- Hitelesítő biztonsági felügyelő (Security Officer /SO/)
- Regisztrációs felügyelő (Registration Officer /RO/)
- rendszer auditor

Az egyes bizalmi munkakörök betöltéséhez szükséges képzettség és gyakorlat:

- biztonsági tisztviselő (IB adminisztrátor, SO):
  - szakirányú közép vagy felsőfokú végzettség,
  - középfokú végzettség esetén legalább három, felsőfokú végzettség esetén legalább egy év informatika biztonsággal összefüggésben szerzett szakmai gyakorlat,
- regisztrációs biztonsági tisztviselő (RO):

- középfokú szakirányú végzettség,
- legalább egy év informatika biztonsággal összefüggésben szerzett szakmai gyakorlat,

♦ működtető adminisztrátor, rendszer auditor:

- középfokú szakirányú végzettség, valamint
- legalább egy év, hasonló munkakörben szerzett szakmai gyakorlat

Az informatika biztonsággal kapcsolatos valamennyi bizalmi munkakört[41] betöltő munkatársra nézve egy személyes továbbképzési terv készül, melyet évente áttekintenek (egyúttal az időközben elvégzett továbbképzési, oktatási anyagokkal kiegészítenek), illetve az adott munkakörhöz tartozó szakmai ismeretek megújulása, változása függvényében aktualizálnak.

A szerepkörökhöz csak fokozott biztonsági ellenőrzéssel lehet személyt rendelni, amelyhez szükséges a szerepkörre kijelölt személy hozzájárulása, ugyanakkor a fokozott ellenőrzés a szerepkör betöltésének alapfeltétele.

A fokozott biztonsági ellenőrzés fontosabb intézkedései:

♦ Újonnan felvett személy csak 1 éves próba idő után töltheti be a szerepkört,

♦ Felvételkor, illetve a szerepkörhöz történő hozzárendeléskor:

- több azonosító dokumentumból történő azonosítás-hitelesítés,
- életrajzi adatok, információk ellenőrzése,
- anyagi helyzet ellenőrzése,
- családi helyzet ellenőrzése,
- személyiség vizsgálat.

A szerepkörhöz történő hozzárendeléskor:

♦ pontos és írásos munkaköri leírást kell átvennie a fölérendelt vezetőtől,

♦ gondoskodni kell a megfelelő helyettesítésről betegség, szabadság, egyéb okú távollét esetére,

♦ titoktartási nyilatkozatot kell a kijelölt személlyel aláíratni, amelyben 3 év titoktartási kötelezettség szerepel a Szolgáltatótól történő kilépés utáni időponttól számítva,

♦ a szükséges mértékű oktatásban kell a kijelölt személyt részesíteni, annak érdekében, hogy a feladat-, felelősség és hatáskörét pontosan megismerje és gyakorolni tudja.

[41] Ez a meghatározás az összes bizalmi munkakörre vonatkozik

Kilépéskor:

- A kilépésről szóló döntés meghozatalakor a kilépő fizikai és logikai belépési és hozzáférési jogosultságait azonnal meg kell szüntetni. A kilépő ezután az informatikai biztonsági menedzser kíséretében léphet be még egyszer a munkahelyi környezetébe, a személyes dolgai elvitele céljából.
- A kilépő személy számítógépes tevékenységét legalább két hétre visszamenőlegesen le kell ellenőrizni.
- Vissza kell venni a Biztonságos aláírás létrehozó eszközét, azonnal és dokumentáltan meg kell semmisíteni azt.
  A kapcsolódó tanúsítvány(oka)t azonnal vissza kell vonni.
- Minden, a kilépőnél levő dokumentációt és ügyiratot vissza kell venni, különös tekintettel a biztonsági és/vagy minősített adatokat információkat tartalmazó anyagokra.
  A visszaadott anyagokról tételes átvételi jegyzőkönyvet kell felvenni.

Nem tölthet be bizalmi munkakört az a személy, aki akár az alap, akár egy időszakos biztonsági ellenőrzésen a „elfogadhatatlanul nagy biztonsági kockázat" minősítést kapja[42].

Az időszakos biztonsági ellenőrzésre rendszeres időnként kerül sor:

- IB adminisztrátorok, SO-k és RO-k esetében 3 évente,
- működtető adminisztrátorok, valamint operátorok esetében 5 évente.

5.3.3. Kiképzési követelmények

A Hitelesítő Központ, a Regisztrációs Iroda, az Ügyfélkapcsolati Iroda és a Help Desk területén dolgozó valamennyi munkatárs felvételét követően, illetve a szolgáltatások indítását megelőzően, a saját munkakörének betöltéséhez szükséges elméleti és gyakorlati alapkiképzésben vesz részt.

Valamennyi munkakörbe való végleges kinevezésnek feltétele az alapkiképzésen való részvétel, s az ezt követő írásos teszten legalább „megfelelő" eredmény elérése.

Rendszerüzemeltetői munkakörben kinevezett (véglegesített) munkatárs a kinevezést követő 3 hónapig, megfelelő gyakorlattal rendelkező kollégával közösen van beosztva (nem lehetséges,

[42] A már bizalmi munkakört betöltő munkatársaktól való, biztonsági okokból történő megválást az alkalmazható legdiszkrétebb módon hajtják végre.

hogy a két egyszerre szolgálatban lévő rendszerüzemeltető mindegyike az adott munkahelyen kezdő).

5.3.4. Továbbképzési gyakoriságok és követelmények

Minden bizalmi munkakört betöltő munkatárs esetében egy személyre szóló éves továbbképzési terv készül. (Ez tartalmazza az arra az évre beütemezett szervezett belső továbbképzéseket, illetve külső tanfolyamokon, egyéb továbbtanulási formákban való ismeretszerzést.) A személyes továbbképzési tervet a humánpolitikai szervezeti egység bevonásával, a Szolgáltató Üzleti Egység vezető évente áttekinti, értékeli és (az érintett munkatárs beleegyezésével) aktualizálja.

Abban az esetben, amikor a szolgáltatásban jelentős változás[43] következik be, valamennyi munkatárs, az őt érintő mélységben továbbképzésben részesül, illetve megkapja a számára szükséges dokumentációkat.[44]

Kisebb változások[45] bekövetkezése előtt a munkatársak írásos tájékoztatást kapnak a változásokról.

5.3.5. Munkabeosztás körforgásának gyakorisága és sorrendje

Körforgás az egyes munkabeosztások között nem valósul meg[46].

5.3.6. A felhatalmazás nélküli tevékenységek büntető következményei

Valamennyi bizalmi munkakört betöltő munkatárs esetén, a munkakörbe kinevezéskor a foglalkoztatási dokumentumok részeként

- írásos tájékoztatást kapott jogszabályi kötelezettségeiről, jogairól, a személyes adatai kezelésére vonatkozó minősítési és kezelési szabályokról,

[43] Jelentős változásnak minősül a szervezeti biztonságpolitika módosulása, a szoftver vagy hardver rendszer változása (upgrade), valamint a kulcs kezelés és biztonság kezelési óvintézkedések változásai.

[44] Attól függően, hogy a bekövetkező jelentős változás előre tervezett volt, vagy váratlanul kellett sort keríteni rá, a továbbképzés illeszkedik az éves továbbképzési tervekbe, vagy rendkívüli módon, soron kívül iktatódik be.

[45] Kisebb változásnak minősül, pl. egy új, kevés tapasztalattal rendelkező munkatárs munkába állása, mely a vele dolgozóktól átmenetileg nagyobb figyelmet és óvatosságot igényel.

[46] Természetesen ez nem jelenti azt, hogy pl. egy operátor, megszerezve a szükséges végzettséget és gyakorlatot, nem „léphet előre" idővel rendszeradminisztrátorrá. Csupán arról van szó, hogy a szakmailag jelentősen eltérő tudást igénylő munkakörök között nincs kötelező, időről időre megvalósuló csere vagy körforgás.

- munkaköri leírást kapott, mely tartalmazta az őt érintő biztonsági feladatokat,
- titoktartási nyilatkozatot írt alá, melyben a biztonsági intézkedések be nem tartásával járó, őt érintő következmények (büntető szankciók) is megfogalmazódtak.

Mindezek tartalmazzák azokat a munkajogi vagy büntető következményeket, melyek a különböző fegyelmi, munkaköri kötelezettség, illetve törvénysértést szankcionálják.

Amennyiben egy munkatárs (gondatlanságból fakadóan vagy szándékosan) megsérti a fenti szabályokat, ellene büntető intézkedéseket hoznak, amelyek az elkövetés módjától és következményétől függően a jutalom megvonástól fegyelmi eljárás indításán és kártérítésen át, egészen a hatósági feljelentésig terjedhet.

5.3.7. A szerződéses alkalmazottakra vonatkozó követelmények

A Szolgáltató bizalmi munkakörben csak vele 1 évnél hosszabb munkaviszonyban álló személyt alkalmaz.

Az egyéb feladatok ellátására, alvállalkozói vagy megbízásos szerződésben foglalkoztatott szerződő személyeket (külső munkavállalókat és ideiglenes alkalmazottakat egyaránt) a Szolgáltató csak az „ellenőrzött beszállítók” listájáról választ. Az ellenőrzött beszállítókkal a Szolgáltató PKI Üzleti Egysége előzetesen írásos megállapodást köt, amelyben vállalja a Szolgáltató biztonságpolitikájának elfogadását.

Valamennyi szerződő fél - még a tényleges munkavégzés megkezdése előtt – titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a munkavégzés során későbbiekben megismerendő üzleti/vállalati titkokat illetéktelen személynek fel nem fedi, s egyéb módon sem hasznosítja. A titoktartási nyilatkozat záró része tartalmazza a megszegése esetén alkalmazandó szankciókat is.

A külső munkavállalók és ideiglenes alkalmazottak szakmai kiképzésben, továbbképzésben nem részesülnek, erre nem kötelezettek[47].

[47] A külső munkavállalókat eleve úgy választják meg, hogy az adott munkafeladathoz minden szakmai ismerettel és gyakorlattal rendelkezzenek. Az ideiglenes alkalmazottak olyan jellegű munkát végeznek, melyhez nincs szükség ki- és továbbképzésre.

5.3.8. A személyzet számára biztosított dokumentációk

A személyzet számára biztosítandó dokumentációt a 9.1 pont sorolja fel.

6. Műszaki biztonsági óvintézkedések

A Szolgáltató megbízható, informatikai biztonság szempontjából értékelt és minősített termékekből álló, egységes informatikai rendszert használ szolgáltatásai nyújtásához.

A rendszert szállítója hitelesítés és időbélyegzés szolgáltatási rendszer kiépítésében jelentős tapasztalatokkal rendelkezik, nemzetközileg elismert technológiát alkalmaz.

6.1. Kulcspár előállítás és telepítés

6.1.1. Kulcs-pár előállítás

A Szolgáltató maga generálja a kulcspárt biztonságos kriptográfiai modulban vagy magán az Aláírás létrehozó eszközön. Nem fogad el az Előfizető által generált Aláírás létrehozó adatot. A Biztonságos aláírás létrehozó eszköz (chip kártya) megszemélyesítése a Szolgáltatónál – fokozott biztonságú környezetben – üzemelő kártya-megszemélyesítő rendszeren történik.

Az Aláírás létrehozó adat elhelyezésére a Szolgáltató csak Tanúsítvány kibocsátással és a kibocsátott Tanúsítvány chip kártyán történő elhelyezésével együtt vállalkozik.

A chip kártya megszemélyesítés szolgáltatáshoz vizuális – egy oldali nyomással történő – grafikus megszemélyesítése is kapcsolódik az Előfizetői Szerződésben meghatározott adattartalommal. A Szolgáltató a Tanúsítványt tartalmazó chip kártyához a Szolgáltató PIN kódot biztosít.

A Szolgáltató saját, tanúsítvány, illetve időbélyeg aláírókulcspár előállítása:

- A Szolgáltatónál történő kulcselőállítást fizikailag védett környezetben (lásd 5.1), SO (lásd 5.2.1) végzi, legalább kettős ellenőrzés[48] mellett. A kulcselőállítás funkció végrehajtására felhatalmazott személyzet körét a Szolgáltató HSzSz-ének még megfelelve, a lehető legkisebbre korlátozza.

[48] Két SO együttes jelenlétével

- A Szolgáltató a kulcselőállítást egy olyan eszközön belül hajtja végre, amely hazai tanúsítvánnyal rendelkezik és szerepel a Hírközlési Felügyelet által jóváhagyott minősített elektronikus aláírási termék listában.
- A Szolgáltató a kulcs előállítását olyan algoritmussal valósítja meg, melyet jogszabály ismer el erre a célra alkalmasnak.[49]

A Szolgáltató által más felek számára előállított kulcspár előállítás:

- A Szolgáltató által saját szervezeti egységei /Címtár, Regisztrációs Iroda/ számára előállított kulcsokat biztonságos módon, egy olyan algoritmussal állítja elő, melyet jogszabály ismer el erre a célra alkalmasnak[50].
- A Szolgáltató által az aláírók számára előállított kulcsokat biztonságos módon, egy olyan algoritmussal állítja elő, melyet jogszabály ismer el erre a célra alkalmasnak [51].
- A Biztonságos aláírás-létrehozó eszköz elkészítését (logikai és fizikai megszemélyesítését) a Szolgáltató ellenőrzi.

A Hitelesítő Központ (CA) az alábbi kulcsokat használja:

- aláíró kulcs az előfizetői tanúsítványok, az RO tanúsítványok, a visszavonási listák és a naplók aláírására,
- PKIX protokollhoz felhasznált kulcs,
- időbélyeg aláíró kulcs.

Valamennyi kulcspárt saját maga generálja, védett kriptográfiai hardver modulban. A generált magánkulcsok a (6.2.4 alatt részletezett) mentést leszámítva, teljes életciklusuk alatt a kriptográfiai hardverekben maradnak, megsemmisítéséig azokat sehová nem kell továbbítani.

A mentéseket, az archivált adatállományokat az SO írja alá.

A Regisztrációs Iroda csak egy fajta kulcspárral rendelkezik, amelyet maga generál és az Aláírás létrehozó adatot Biztonságos aláírás létrehozó eszközön helyezi el. A generált magánkulcs teljes életciklusa alatt a kriptográfiai hardverben marad, megsemmisítéséig azt sehová nem kell továbbítani.

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

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

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

A végfelhasználók kulcspárjait a Regisztrációs Iroda kezdeményezésére a PKI alkalmazás generálja. A minősített aláíró kulcs védett csatornán átkerül a Biztonságos aláírás-létrehozó eszközre, s előállítása helyén azonnal és minden későbbi reprodukálást kizáró módon megsemmisül. Ezt követően a magánkulcs teljes életciklusa alatt csak a Biztonságos aláírás-létrehozó eszközön (intelligens kártya) marad, a végfelhasználókhoz való továbbítása magának az intelligens kártyának a végfelhasználóhoz történő továbbítását jelenti.

Az időbélyeg aláíró kulcsot az időbélyegző központ szerves részét képező tanúsított hardver kriptográfiai modul generálja és tárolja. A kulcs a megsemmisítésig ezen eszközben marad.

MTT+BALE esetén a végfelhasználó kulcspárjait a Regisztrációs Iroda kezdeményezésére a PKI alkalmazás generálja egy védett kriptográfiai hardver modulban.

6.1.2. Az Aláírás létrehozó adat felhasználóhoz történő eljuttatása

A Szolgáltató, amikor kulcsokat generál más felek (pl. Regisztrációs Iroda 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 a Biztonságos aláírás-létrehozó eszköz elkészítését,
- a Szolgáltató a nem megszemélyesített Biztonságos aláírás-létrehozó eszközt is biztonságosan tárolja.
- a Szolgáltató megszemélyesíti a Biztonságos aláírás-létrehozó eszközt és biztonságosan tárolja.
- a Szolgáltató biztonságosan ellenőrzi a Biztonságos aláírás-létrehozó eszköz kiiktatását és újraaktivizálását,

- a Szolgáltató a Biztonságos aláírás-létrehozó eszköz aktivizálási adatait (PIN kód) biztonságosan készíti el és a Biztonságos aláírás-létrehozó eszköztől elkülönítve személyesen adja át vagy biztonságosan postázza az Előfizetőnek.

Az Előfizető vagy az Aláíró számára:

- olyan algoritmus felhasználásával kell előállítaniuk az Aláíró kulcsait, melyet jogszabály a tanúsítványtípusban azonosított kulcshasználatra megfelelőnek ismer el,
- olyan kulcshosszúságot és algoritmust kell alkalmazniuk, amelyet jogszabály a tanúsítványtípusban azonosított kulcshasználatra megfelelőnek ismer el.

Egy Előfizetőnek a megszemélyesített és legyártott chip kártyákat személyesen kell átvennie, az átvétel írásos elismerésével.

Az átadás során átadásra kerül:

- kulcshordozó eszköz és rajta a magánkulcs, illetve a Tanúsítvány,
- az aláírt regisztrációs űrlap egy példánya,
- a tájékoztató füzet,
- az aláírt Előfizetői Szerződés egy példánya.

A kulcshordozó eszköz átvételének megtagadása visszavonási kérelemnek számít.

6.1.3. Aláírás ellenőrző adat eljuttatása a tanúsítvány kibocsátóhoz

Az Előfizető Tanúsítványba foglalandó nyilvános kulcs a Regisztrációs Irodától tanúsítványigénylés formában, a Regisztrációs Iroda magánkulcsával elektronikusan aláírt elektronikus üzenetben kerül a Hitelesítő Központhoz.

6.1.4. Hitelesítő Szervezet Aláírás ellenőrző adatának eljuttatása a felhasználókhoz

A Hitelesítő és az időbélyegző központok Root CA által aláírt nyilvános kulcsait saját Címtárában teszi mindenki számára elérhetővé[52].

[52] Mivel a Hitelesítő Központ nem önaláírt, hanem a Root CA által aláírt tanúsítványt alkalmaz, ezért a saját nyilvános kulcsának közzétételére használt módszer mindenki számára (aki rendelkezik a Root CA nyilvános, tanúsítvány ellenőrzéshez szükséges kulcsával) megbízható.

Az itt közzétett Tanúsítvány ellenőrzéséhez szükséges Root CA nyilvános kulcs közzététel az alábbi módon valósul meg:

- A hitelesítő, illetve az időbélyegző központ a Root CA-tól egy tokenen kapja meg a nyilvános kulcsot, amelyet két SO személyesen hoz el a Root CA-tól.
- A Regisztrációs Iroda a Root CA-tól egy tokenen kapja meg a nyilvános kulcsot, amelyet két SO személyesen hoz el a Root CA-tól.
- Az aláírók a Root CA nyilvános kulcsát a Regisztrációs Iroda által feltöltött Aláírás létrehozó eszközön (intelligens kártyán) kapják meg a személyes átvételkor.

A fentieken kívül a Root CA nyilvános kulcsa megszerezhető, illetve ellenőrizhető közvetlenül is, mivel a Szolgáltató CA közzéteszi a Root CA nyilvános kulcsát a http://www.mavinformatika.hu/ca/ web lapon keresztül.

Az Root, a produktív hitelesítő és az időbélyegző központok nyilvános kulcsai azok Tanúsítványába foglalva a Címtárba íródnak. A hitelesítő központok tanúsítványai felkerülnek a Szolgáltató nyilvános web oldalaira is a **http://www.mavinformatika.hu/ca/** címen.

A tanúsítványok letölthetők és a felhasználó kliens-alkalmazásába installálhatóak. A Szolgáltató Ügyfélkapcsolati Irodája, kérés esetén, telefonon is rendelkezésre áll a digitális lenyomat egyeztetése céljából.

6.1.5. Kulcs méretek

Az 1. szintű Hitelesítés Központ ("Root") aláíró kulcsának mérete:	2048 bit
A 2. szintű Hitelesítő Központ aláíró kulcsainak mérete:	2048 bit
Az időbélyegző központ aláíró kulcsának mérete:	2048 bit
A 2. szintű Hitelesítő Központ kommunikációs kulcsának mérete:	1024 bit
A Regisztrációs Iroda kommunikációs kulcsának mérete:	1024 bit

A szerződéses viszonyban álló aláírók
aláíró RSA kulcsainak mérete: 1024 bit

6.1.6. Előfizetői Aláírás ellenőrző adat előállításához használt paraméterek előállítása

A Hitelesítő Központ elektronikus és időbélyegző aláírásra az RSA[53] algoritmust használja.

Az aláírók számára kibocsátott tanúsítványok az RSA aláíró algoritmusokhoz használhatók.

A szerződéses viszonyban álló aláírók esetében a kulcsgenerálást a Biztonságos aláírást létrehozó eszköz on board elvégzi vagy a PKI alkalmazás.

Előfizetői Aláírás ellenőrző adat előállításához használt paraméterek megfelelőségét a hazai tanúsító szervezet és a gyártó tanúsítják. A kapcsolódó dokumentumok a Szolgáltatónál megtekinthetők.

6.1.7. Szoftveres / hardveres kulcsgenerálás

A Szolgáltatóra vonatkozóan CC EAL4 szintű követelményeknek megfelelő hardver modulban vagy Biztonságos aláírás létrehozó eszközben történik a kulcsgenerálás, amelyet a Szolgáltató minősített tanúsítvánnyal (MTT+BALE) hitelesít.

A Szolgáltató az időbélyeg aláíró kulcsot az időbélyegző központ Biztonságos aláírás létrehozó eszközében (HSM[54]) generálja, tárolja. Az időbélyeg aláíró kulcs tanúsítványát a Szolgáltató root CA-ja hitelesíti.

Az előfizetői kulcsokat a Szolgáltató vagy Biztonságos aláírást létrehozó eszközben vagy PKI alkalmazással hozza létre.

6.1.8. Kulcs felhasználási célok

A Szolgáltató Előfizető részére kulcspárt elektronikus aláírási célra bocsát ki.

53 Az RSA algoritmust (Rivest, Shamir and Adleman Algorithm) az alábbi szabvány írja le részletesen: International Organization for Standardization, “ISO/IEC 14888-3: Information technology - Security techniques - Digital signatures with appendix - Part 3: Certificate-based mechanisms,” 1999.

54 Hardware Security Modul

Az előfizetők részére kibocsátott tanúsítványok bővítmény (Extension) részében található „KeyUsage” mezőbe elektronikus aláírás felhasználási célként a „nonRepudiation” kulcshasználati módnak megfelelő kijelölést kell alkalmazni.

A kulcspár kizárólag arra a célra használható, amelyre a Szolgáltató kibocsátotta, a HSzSznek és az Előfizetői Szerződés feltételeinek megfelelően.

A Szolgáltató Üzleti Egység szervezeti egységei esetében a „Key Usage” mezők lehetséges (egyúttal kötelezően kitöltendő) értékeit a következő táblázatok mutatják.

Hitelesítő Központ

Kulcs megnevezése	„Key Usage” mező értéke	Kritikus/Nem kritikus
CA aláíró kulcsa	KeyCertSign, cRLSign	**K**
Időbélyegző központ aláíró kulcsa	nonRepudiaton	**K**
	Az „Extended Key Usage” mezőbe: timeStamping	**K**
A CA PKIX kommunikációs kulcs (Regisztrációs Irodával való biztonságos kommunikáció megteremtésére)	DigitalSign, DataEncipherment, KeyEncipherment	**K**

Regisztrációs Iroda

Kulcs megnevezése	„kulcs használati” mező értéke	Kritikus/Nem kritikus
CA PKIX kommunikációs kulcs (a Hitelesítő Központtal való biztonságos kommunikáció megteremtésére)	DigitalSign, DataEncipherment, KeyEncipherment	**K**

6.2. Aláírás létrehozó adat védelme

6.2.1. Kriptográfiai modulra vonatkozó szabványok

Az előfizetők Aláírás létrehozó adatának tárolására Szolgáltató olyan eszközt bocsát ki MTT+BALE esetén, amely teljesíti a CC EAL4 követelményeket

Az Aláírás létrehozó adatot a Szolgáltató PIN kóddal védve bocsátja ki. Az Aláírás létrehozó adat dokumentált átvétele után az Előfizető felelős a Biztonságos aláírás létrehozó eszköz, az Aláírás létrehozó adat, valamint a PIN kód védelméért.

A Szolgáltató saját tanúsítvány és időbélyeg aláíró kulcsainak tárolására Biztonságos kriptográfiai modult alkalmaz, amely rendelkezik hazai tanúsítással és a HIF által regisztrált kriptográfiai modulok listájában szerepel.

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

A Szolgáltatónál egyedül a Hitelesítő Központban alkalmazzák az „n-ből m" ellenőrzést a Root CA kulcsgondozási funkcióinak aktivizálásánál.

A részekre osztott titok a Root CA aláíró kulcsot 6 részre osztják, melyből 3-nak kell együttesen jelen lennie a sikeres visszaállításhoz /n=6, m=3/.

6.2.3. Aláírás létrehozó adat letét

A Szolgáltató nem nyújt magánkulcs letétszolgáltatást. Az előfizetői Aláírás létrehozó adatot, vagy annak előállítására, visszafejtésére alkalmas programot, adatot nem tárol.

6.2.4. Aláírás létrehozó adat mentése, duplikálása

A Szolgáltató az Előfizető aláírói Aláírás létrehozó adatot semmilyen formában nem menti, vagy tárolja.

A Szolgáltatónál a Hitelesítő Központ aláíró magánkulcsai[55] duplikálásra, klónozásra kerülnek.

A mentés funkció kiváltásához speciális eszközök kerülnek alkalmazásra. A mentés rejtjeles formában hajtódik végre.

6.2.5. Aláírás létrehozó adat archiválása

Szolgáltató Aláírás létrehozó adatot nem archivál.

55 A kriptográfiai hardver modul (tanúsítványokat, illetve visszavonási listákat aláíró) magánkulcsai.

6.2.6. Aláírás létrehozó adat kriptográfiai modulba helyezése

A Hitelesítő Központ biztonságos kriptográfiai modulja maga generálja saját aláíró és kommunikációs kulcspárjait (lásd 6.1.1), s a magánkulcs nyílt (titkosítatlan) formában nem hagyja el a modult.

A Hitelesítő Központ időbélyegző központjának HSM egysége generálja és tárolja az időbélyeg aláíró kulcsot, amelynek Tanúsítványát a Root CA írja alá.

A magánkulcsok csak a modul (token) mentésénél, duplikálásánál hagyják el a modult. A mentési (klón) modulba ilyen esetekben a magánkulcs rejtjeles védelem alatt másolódik át.

A Regisztrációs Iroda számára az PKI biztonsági felügyelő(SO) generálja kulcspárjait BALE chip kártyán, és a magánkulcsok semmilyen körülmények között nem hagyják el a modulokat. (Tehát soha nem kell kívülről bejuttatni azokat.)

A végfelhasználók aláíró kulcspárjait a Regisztrációs Iroda generálja BALE chip kártyán vagy a PKI alkalmazással. Ezt követően a magánkulcsok teljes életciklusuk során nem hagyják el az intelligens kártyát MTT+BALE esetén.

6.2.7. Aláírás létrehozó adat aktiválása

Az előfizetői Aláírás létrehozó adat aktiválása a felhasználó által történik a jelszó vagy PIN kód megadásával, azokban az esetekben, amikor az Aláírás létrehozó adat használatára szükség van. Az Aláírás létrehozó eszközt az Aláírás létrehozó adat aktiváláskor sem hagyja el, az eszközről leolvasni nem lehet.

6.2.8. Aláírás létrehozó adat deaktiválása

Az előfizetői Aláírás létrehozó adatok deaktiválását a felhasználó alkalmazása végzi az Aláíró kijelentkezésekor, vagy amikor az Aláíró az Aláírás létrehozó eszközt eltávolítja az olvasóból.

6.2.9. Aláírás létrehozó adat megsemmisítése

Az előfizetői Aláírás létrehozó adat lejárta után az Aláírás létrehozó eszköz fizikai megsemmisítését az Előfizetőnek saját felelősségi körében úgy kell elvégezni, hogy az semmilyen körülmények között ne legyen újra felhasználható.

A szolgáltatói Aláírás létrehozó adatok megsemmisítése a Szolgáltató kötelessége.

6.3. Kulcs-pár kezelés egyéb aspektusai

6.3.1. Aláírás ellenőrző adat archiválása

Az operátorok minden a Szolgáltató által előállított Tanúsítványt archiválnak, az alábbi időszakra:

- nem előfizetői tanúsítványok: az érvényesség lejártától számított 10 évig,
- előfizetői tanúsítványok: az érvényesség lejártától számított 1 évig.

A nyilvános kulcsok archiválásáért az operátorok a felelősek (lásd 5.2.1).

Az archiválás (az integritásellenőrzést biztosító lenyomatértékekkel együtt) egyszer írható CD-kre történik, amelyeket a Szolgáltató a Biztonsági Adattárban és a katasztrófa helyszínen tárol a megőrzési idő végéig.

6.3.2. Aláírás létrehozó és ellenőrző adatok felhasználási ideje

A Root CA aláíró kulcshoz tartozó Tanúsítvány érvényességi ideje:	10 év
Az időbélyegző központ aláíró kulcshoz tartozó Tanúsítvány érvényességi ideje:	10 év
A Produktív CA aláíró kulcsához tartozó Tanúsítvány érvényességi ideje:	3 év
A RO kommunikációs kulcsához tartozó Tanúsítvány érvényességi ideje:	max. 3 év
Az előfizetői aláírók aláíró kulcsához tartozó Tanúsítvány érvényességi ideje:	1 év

Valamennyi fenti Tanúsítvány (és a benne foglalt nyilvános kulcs) érvényességének kezdete a kibocsátás időpontjával egyezik meg.

Valamennyi fenti Tanúsítvány esetén a megfelelő magánkulcs érvényességi ideje megegyezik a Tanúsítvány érvényességi idejével.

6.4. Aktiválási adatok

6.4.1. Aktiválási adatok generálása és installációja

A Regisztrációs Iroda az általa kibocsátott Aláírás-létrehozó eszközök aktivizáló adatait (PIN kódjait) a PKI alkalmazás állítja elő.

6.4.2. Aktiválási adatok védelme

A Regisztrációs Iroda az általa kibocsátott Aláírás-létrehozó eszközök aktivizáló adatait (PIN kódjait) műszaki[56] és szervezési[57] intézkedésekkel védi az Előfizetőnek vagy az Aláírónak történő átadásig, majd a Biztonságos aláírás-létrehozó eszköztől elkülönítve[58] adja át vagy biztonságosan postázza.

A Szolgáltató a Biztonságos Aláírás-létrehozó eszköz használatához szükséges, az Aláíró hozzáférési jogosultságát ellenőrző adatot (PIN-kódot) csak abból a célból rögzítheti, hogy azt a szolgáltatást igénybe vevő személy számára - másolat megőrzése nélkül - átadhassa[59].

Az átvétel tán az Aláíró a saját munkaállomásán megváltoztathatja a PIN kódot, amelyhez megfelelő ügynök programmal (CSP) kell rendelkeznie.

Az Előfizető a későbbiekben is bármikor megváltoztathatja a PIN kódját.

Előfizetői Aláírás létrehozó adatának kizárólag csak az Aláíró által történő birtoklása az alapvető feltétel az elektronikusan aláírt adat, dokumentum hitelességének biztosítására. Emiatt az Előfizetőnek saját felelősségi körében kell biztosítania az aktivizáló adat kizárólagos birtoklá-

[56] A PIN kódok generálása, kinyomtatása és borítékolása egy zárt láncú, automatikus, ember által megszakíthatatlan folyamattal történik.

[57] A címzettekhez történő továbbításig, a rendszerüzemeltetők gondoskodnak a beborítékolt PIN kódok biztonságos tárolásáról.

[58] Az elkülönítés úgy van biztosítva, hogy a PIN kódok és intelligens kártyák szétosztása, illetve átadása külön lezárt borítékokban történik.

[59] 16/2001. (IX. 1.) MeHVM rendelet 39§, 4. bek. szerint.

sát. Amennyiben ez sérül vagy elveszik, illetve ennek alapos gyanúja fennáll, akkor az Előfizetőnek ezt haladéktalanul jelentenie kell az Ügyfélkapcsolati Irodánál vagy az Ügyfélszolgálatnál, amely azonnal intézkedik a Tanúsítvány visszavonásáról.

Az Előfizető Aláírás létrehozó adatának aktiválási adatát a Szolgáltató az Aláírás létrehozó adat előállítása után megsemmisíti, büntetőjogi felelőssége mellett nem hozza harmadik fél tudomására.

A Szolgáltató a saját aktiválási adatait a MeH 12. ajánlás által meghatározott fokozott biztonsági szinten védi a 2.8 fejezetben (Bizalmasság – Adatkezelési szabályzat), a 2.84.6 fejezetben (Biztonsági audit eljárások), 4.65. fejezetben (Fizikai, eljárásrendi, és humán biztonsági szabályozások), és a 6.5 fejezetben (Számítógép biztonsági szabályok) meghatározott biztonsági intézkedésekkel.

6.4.3. Aktiválási adatok egyéb aspektusai

Az előfizetői aktiválási adatát Szolgáltató nem tárolja, és nem állítja újra elő az Előfizető, harmadik fél, vagy hatóság kifejezett kérése esetén sem.

Az aktiváló adat elvesztése, elfelejtése vagy illetéktelen kezekbe történő jutása esetén minden esetben új kulcspárt és aktiválási adatot kell előállítani.

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 meg.

A Szolgáltató olyan megbízható informatikai rendszert alkalmaz, mely az alábbi termékeken alapul:

- operációs rendszer,
- PKI alkalmazás,
- időbélyegzés alkalmazás,
- kriptográfiai hardver modulok,

- tűzfalak,
- behatolás detektorok.

Az operációs rendszerek által megvalósított biztonsági funkciók az alábbiak:

- biztonsági naplózás (a felhasználói hozzáférések és tevékenységek rögzítése, a biztonsági napló védelme, az ahhoz való hozzáférés rendszervizsgáló szerepkörre korlátozása),
- a felhasználói adatok védelme (a hozzáférés ellenőrzési szabályok alapjainak érvényre juttatása /rendszer fájlok védelme, a felhasználói adatok csak alkalmazáson keresztüli elérésének biztosítása/, a tárolt adatok sértetlenségének védelme /beleértve a vírusok, káros és engedély nélküli szoftverek elleni védekezés támogatását is/, a maradvány információ védelmének megvalósítása),
- azonosítás és hitelesítés (a felhasználók azonosítása és hitelesítése, az operációs rendszer által biztosított funkciók elérésének sikeres hitelesítéshez kötése),
- biztonságkezelés (a biztonsági szerepkörök kezelése, a hozzáférési jogosultságok szerepkörök szerinti beállítása, módosítása),
- a biztonsági funkciók megbízható védelme (alap biztonsági tesztelés végrehajtása, biztonságos állapot megőrzése hiba esetén, a hozzáférés ellenőrzés megkerülhetetlenségének biztosítása, a különböző alkalmazói folyamatok által használt tartományok elkülönítése).

A PKI alkalmazás által megvalósított biztonsági funkciók az alábbiak:

- biztonsági naplózás (a rendszerüzemeltetői hozzáférések és tevékenységek rögzítése),
- kommunikáció (a Hitelesítő Központ és a Regisztrációs Iroda közötti kommunikáció bizalmasságának, sértetlenségének és hitelességének biztosítása /a kriptográfiai hardver modulok megfelelő funkcióinak aktivizálásával/),
- a felhasználói adatok védelme (a hozzáférés ellenőrzési szabályok érvényre juttatása /az elindított alkalmazások csak a jogosultságnak megfelelő funkciók elérhetőségét biztosítják/, a maradvány információ védelmének támogatása),
- azonosítás és hitelesítés (a rendszerüzemeltetők azonosítása, hitelesítése, az alkalmazások által biztosított funkciók elérésének sikeres hitelesítéshez kötése).

Az időbélyegzés alkalmazás által megvalósított biztonsági funkciók az alábbiak:

- biztonsági naplózás (a rendszerüzemeltetői hozzáférések és tevékenységek, az időbélyegzés lépéseinek rögzítése és az időszinkronizálás eseményei és pontossága),

- kommunikáció (az időbélyegző központ és az időbélyeg felhasználó ügyfelek kommunikáció bizalmasságának, sértetlenségének és hitelességének biztosítása SSL kapcsolattal),
- az operációs rendszer és alkalmazás szintű adatok védelme fokozott erősségű azonosítás-hitelesítéssel, hozzáférési jog csak az üzemeltetési adminisztrátor és a kijelölt SO részére.
- Az időbélyeg aláíró kulcs bizalmasságának, hitelességének és sértetlenségének fokozott szintű fizikai védelmét a Bizalmi Központban történő generálás és tárolás biztosítja. A külső hálózat felőli fenyegetések ellen védelmet nyújt a többszörös tűzfal rendszer és az időbélyegző szerverek külön biztonsági zónában történő üzemeltetése.
- Az időbélyegző szerver belső órájának pontossága folyamatos ellenőrzés alatt áll. A pontossági tartományból történő kilépés esetén az időbélyegző szolgáltatás leáll és a hiba kijavításáig minden további kérésre hibaüzenet kerül kiküldésre az előfizetők felé.
- A külső szinkronizáló négy külső, független időforrásból történik.
- A külső szinkronizáló órajelek hitelességét az időbélyegző informatikai rendszer indításakor egy erre a célra létrehozott bizottság tanúsítja. A bizottság minden olyan esetben összehívásra kerül, amikor a szinkronizáló órajelek hitelességének sérülésére alapos gyanú merül fel. Ilyenkor a bizottság ellenőrzi az órajelek hitelességét, amelyhez egy független GSM kapcsolaton keresztül lekérdezett UTC idő szolgál referenciaként.
- Az időbélyegzés szolgáltatás 99,5%-os rendelkezésre állását a meleg tartalékolt időbélyegző szerverek, valamint azoknak a magas rendelkezésre állást biztosító felügyelő és vezérlő rendszerbe történt integrálása biztosítja.

A kriptográfiai hardver modulok által megvalósított biztonsági funkciók az alábbiak:

- biztonsági naplózás (a saját funkcióihoz való hozzáférések rögzítése, a saját belső biztonsági napló védelme, az ehhez való hozzáférés rendszervizsgáló szerepkörre korlátozása),
- kriptográfiai támogatás (kriptográfiai kulcsok generálása, védelme és megsemmisítése; bizalmasságot, sértetlenséget, hitelességet és letagadhatatlanságot biztosító kriptográfiai eljárások megvalósítása),
- a felhasználói adatok védelme (a saját hozzáférés ellenőrzési szabályok érvényre juttatása),
- azonosítás és hitelesítés (a saját felhasználók /biztonsági tisztviselők vagy rendszerüzemeltetők/ azonosítása, hitelesítése, a saját funkciók elérésének sikeres hitelesítéshez kötése),

- biztonságkezelés (saját biztonsági szerepkörök kezelése, a hozzáférési jogosultságok szerepkörök szerinti beállítása, módosítása),
- a biztonsági funkciók megbízható védelme (saját működés biztonsági tesztelése, biztonságos állapot megőrzése hiba esetén, a hozzáférés ellenőrzés megkerülhetetlenségének biztosítása),
- megbízható út/csatorna (megbízható útvonal kiépítése a magát hitelesítő felhasználóval, mely alkalmas az átvitt adatok illetéktelen felfedésének és módosításának megakadályozására).

A tűzfal és a behatolásdetektáló által megvalósított biztonsági funkciók az alábbiak:

- biztonsági naplózás (a hálózati kommunikáció naplózása, a biztonsági napló védelme, az ahhoz való hozzáférés rendszervizsgáló szerepkörre korlátozása, a napló folyamatos elemzése: biztonsági riasztások és automatikus válaszok megvalósítása),
- a felhasználói adatok védelme (az információ áramlás ellenőrzési szabályok érvényre juttatása /szűrés, a tiltott információ áramlás megakadályozása, megfigyelése),
- azonosítás és hitelesítés (a saját felhasználók /hálózati adminisztrátorok/ azonosítása, hitelesítése, a saját funkciók elérésének sikeres hitelesítéshez kötése),
- a biztonsági funkciók megbízható védelme (az információ áramlás ellenőrzés megkerülhetetlenségének biztosítása),

6.5.2. Számítógép biztonsági értékelések

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 EAL4 biztonsági osztályok követelményeivel.

A számítógép biztonsági értékelések rendszerét a 3. táblázat mutatja.

Biztonsági ellenőrzés típusa		Végzi	Rendszeresség
Operatív	IT infrastruktúra	Informatikai biztonsági adminisztrátor	Naponta
	PKI alkalmazás	Rendszer auditor	Naponta

Belső ellenőrzés	IT infrastruktúra	Informatikai biztonsági menedzser	Félévente egyszer
	PKI alkalmazás	Hitelesítési Politika és Szabályozási Csoport	Félévente egyszer
Külső ellenőrzés	IT infrastruktúra	Külső auditor	Évente egyszer
	PKI alkalmazás	Külső auditor	Évente egyszer

3. táblázat

6.6. Életciklus technikai szabályok

6.6.1. Rendszerfejlesztési szabályok

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, a működtetés és menedzselés és a visszavonás/rekonstrukció ciklus időszakok feladatait és az alkalmazott módszertanokat.

6.6.2. Biztonságkezelési szabályok

A biztonságkezelési szabályok a Szolgáltató társasági szintű Informatikai biztonságpolitikája, valamint a társasági és a rendszer szintű Informatikai Biztonsági Szabályzatok tartalmazzák. A Szolgáltató hitelesítés és időbélyegzés 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. Az életciklus biztonsági értékelések a 3. táblázat szerinti rendszerben történnek.

6.7. Hálózati biztonsági szabályok

A Szolgáltató hitelesítés szolgáltatás támogató informatikai rendszere fokozott biztonsági osztályba sorolt, a hálózati védelmi intézkedések ennek a biztonsági szintnek megfelelőek.

A Szolgáltató társasági szintű informatikai, valamint a hálózati biztonságpolitikájának és biztonsági architektúrájának megfelelően a Hitelesítő Központ és a Regisztrációs Iroda közötti kommunikáció (belső hálózat) PKIX kapcsolattal védett a bizalmasság, sértetlenség és letagadhatatlanság elvesztése ellen. A magas szintű védelmet hardver kriptográfiai modulok biztosítják.

A Szolgáltató Hitelesítés szolgáltatást és időbélyegzést támogató informatikai rendszerénél a védett belső és a külső hálózatok biztonságos elválasztását tűzfal és betörés figyelő rendszer (IDS) biztosítja.

A Hitelesítő Központ közvetlen külső kommunikációt nem folytat a végfelhasználókkal.

6.8. Kriptográfiai modul ellenőrzése

A kriptográfiai modulok ellenőrzik az illetéktelen beavatkozási kísérleteket. Amennyiben ilyet detektál, akkor:

- a memóriájában levő magánkulcsot törli,
- a modul saját tanúsítványa is törlésre kerül és ezzel a modul használhatatlanná válik.

7. Tanúsítvány és kulcs-visszavonási profil

Az ebben a fejezetben bemutatott minősített tanúsítvány és kulcs-visszavonási profilok megfelelnek a 2/2002 (IV.26.) MeHVM irányelvnek, az ITU-T X.509 szabvány 3. változatának, az EU ETSI TS 101 862 (*Minősített tanúsítvány profil*) szabványnak és az RFC 3039 (*Internet X.509 Nyilvános kulcsú infrastruktúra – Minősített tanúsítvány profil*) Internet szabványnak. Az alkalmazott minősített tanúsítványtípus mezői és azok értelmezése e szabványokat követi.

7.1. Tanúsítvány profil

7.1.1. Alap mezők

A Szolgáltató által kibocsátott előfizetői tanúsítványok alap mezői a következők:

Mezőnév	**Érték vagy szabály**
Verzió *Version*	Szolgáltató az RFC 2459-nek megfelelő tanúsítványokat bocsát ki. Szolgáltató a kibocsátott tanúsítványok „Version” mezőjébe V3 értéket ír.
Sorozatszám *Serial Number*	A kibocsátó Hitelesítő Központon belül egyedi szám, 12 karakter hosszúságú.
Algoritmus azonosító *Signature Algorithm Identifier*	Szolgáltató Tanúsítványt hitelesítő elektronikus aláírásának algoritmus azonosítója, pl. sha1WithRSAEncryption
Aláírás *Signature*	Szolgáltató Tanúsítványt hitelesítő elektronikus aláírása az RFC 2459 szerint generálva és kódolva.
Kibocsátó *Issuer*	A Tanúsítványt kibocsátó Hitelesítő Központ és egység egyedi azonosítója egyedi X.500 név formátumot szerint, UTF8String formátumban.
Érvényesség *Valid From & Valid To*	A Tanúsítvány érvényességének kezdete és vége. UTC szerinti érték, az RFC 2459 szerinti kódolással.

Mezőnév	Érték vagy szabály
Tulajdonosazonosító *Subject*	Tulajdonos egyedi neve egyedi X.500 név formátumot szerint, UTF8String formátumban.
A Tulajdonos nyilvános kulcsának algoritmus azonosítója *Subject Public Key Algorithm Identifier*	Alany nyilvános kulcs algoritmusának azonosítója, pl. rsaEncryption
A Tulajdonos nyilvános kulcsa *Subject Public Key Value*	A Tulajdonos nyilvános kulcsa.
A Kibocsátó egyedi azonosítója *Issuer Unique Identifier*	Nem kitöltött.
A Tulajdonosegyedi azonosítója *Subject Unique Identifier*	Nem kitöltött.

7.1.2. Tanúsítvány kiterjesztések

A Szolgáltató az ITU X.509 szabvány 3. változatának, az EU ETSI TS 101 862 és az RFC 3039 szabványoknak megfelelő tanúsítvány kiterjesztéseket támogatja.

Mezőnév	Érték vagy szabály	Kritikus
Tanúsítvány-típusok *Certificate Policies*	PolicyIdentifier = 1.3.6.1.4.1.14868.2.2.1 (MTT esetén) 1.3.6.1.4.1.14868.2.2.2 (MTT+BALE esetén) PolicyQualifier = http://cps.trust-sign.hu UserNotice = ”*A tanusítvany ertelmezesehez es elfogadasahoz a Szolgaltato HSzSz-eben foglaltak szerint kell eljarni, amely megtalalhato a következo Intenetes web oldalon:* http://www.trust-sign.hu*”* *„Ez a (XXX)[60] minositett tanusitvany a MAV INFORMATIKA Kft. Trust&Sign szolgáltatása keretében lett kibocsátva”*	Igen
Alapvető megkötések *Basic Constraints*	Subject type = End Entity Path Length Constraint = None	Nem

[60] Meg kell adni a minősített tanúsítvány típusát. XXX=MTT vagy XXX=MTT+BALE, a kiadott Tanúsítvány típusától függően. Ezen szöveg alapján a nem szakképzett Érintett fél is azonosítani tudja a Tanúsítvány típusát.

Mezőnév	Érték vagy szabály	Kritikus
Kulcshasználat *Key Usage*	Előfizetői vagy időbélyeg aláíró kulcs használat NonRepudiation CA aláíró kulcsa KeyCertSign, CrlSign RO és CA kommunikációs kulcsok DigitalSign, DataEnchipherment, KeyEncxhipherment	Igen
	Időbélyegzés esetén az „Extended Key Usage” mezőbe: timeStamping	Igen
CRL szétosztási pont *CRL Distribution Points*	http://crl.trust-sign.hu/QCA.crl	Nem
Minősített Tanúsítvány Nyilatkozatok[61] *Qualified Certificate Statements*		
Megfelelőség *QC Compliance* OID:0.4.0.1862.1.1		*Nem*
Tranzakciós limit *Transaction limit* OID:0.4.0.1862.1.2	QcEuLimitValue ::= MonetaryValue MonetaryValue::= SEQUENCE { currency Iso4217CurrencyCode, amount INTEGER, exponent INTEGER} value = amount * 10^exponent	*Nem*
Adat megőrzési idő *Retention time of data* OID:0.4.0.1862.1.3	QcEuRetentionPeriod ::= INTEGER(=10)	Nem

A Szolgáltató által kibocsátott tanúsítványok álnevet tartalmazhatnak.

A kiterjesztési mezők 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.

[61] A minősített tanúsítvány 2/2002 MeHVM irányelvnek és az EU ETSI TS 101 862 szabványnak megfelelő kiterjesztése

7.2. Kulcs-visszavonási profil

A szolgáltató által kibocsátott visszavonási listák alap mezői a következők:

Mezőnév	Érték vagy szabály
Verzió *Version*	A visszavonási lista az ITU-T X.509 ajánlás hányadik verziójának felel meg (lásd 7.2.1 alfejezet).
Algoritmus azonosító *Signature Algorithm Identifier*	Szolgáltató visszavonási listát hitelesítő elektronikus aláírásának algoritmus azonosítója: sha1RSA (OID=1.2.840.113549.1.1.5).
Aláírás *Signature*	Szolgáltató visszavonási listát hitelesítő elektronikus aláírása az RFC 2459 szerint generálva és kódolva.
Kibocsátó *Issuer*	A visszavonási listát kibocsátó hitelesítő szervezet és egység egyedi azonosítója.
Hatályba lépés *Effective Date*	A visszavonási lista hatályba lépésének kezdete. A szolgáltató által kibocsátott tanúsítványok esetében ez megegyezik a kibocsátás idejével. UTC szerinti érték, az RFC 2459 szerinti kódolással.
Következő kibocsátás *Next Update*	A következő visszavonási lista kibocsátásának ideje. UTC szerinti érték, az RFC 2459 szerinti kódolással.
Visszavont tanúsítványok *Revoked Certificates*	A visszavont tanúsítványok listája a Tanúsítvány sorozatszámával és a visszavonás idejével.

A Szolgáltató a következő referencia UTC időforrásokat használja: */ dr-zaius.cs.wisch.edu; carl.cmr.gov; proxy.cc.vt.edu; odp-sun3.tamu.edu; 148.6.0.1. Ezek „Stratum" 1-es és 2-es besorolásúak.*

7.2.1. Verzió szám(ok)

A Szolgáltató ITU-T X.509 ajánlás 2. verziója szerinti tanúsítvány visszavonási listákat bocsát ki.

7.2.2. „Tanúsítvány visszavonási lista” és „Tanúsítvány visszavonási lista bejegyzési” kiterjesztések

A Szolgáltató által használt visszavonás bejegyzési kiterjesztések a következők:

Mezőnév	Érték vagy szabály	Kritikus
Visszavonás oka *reasonCode*	A visszavonás oka	Nem
Érvénytelenség ideje *Invalidity Date*	A magánkulcs megbízhatatlanná válásának ideje	Nem

Szolgáltató a kiterjesztéseket nem köteles kitölteni.

A Szolgáltató által kitöltött visszavonási lista kiterjesztések a következők:

Mezőnév	Érték vagy szabály	Kritikus
CRL sorozatszám *CRL number*	A visszavonási lista egyesével növekvő sorozatszáma	Nem

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.

7.3. Időbélyeg profil

A Szolgáltató által kibocsátott időbélyegek szerkezete követi az RFC3161 szabványt és az ETSI ET 102 023 szabvány 7.3.1 pontjában előírtakat.

Mezőnév		Érték
Verzió	*Version*	v1

Mezőnév		Érték
ISzP azonosító (OID)		1.3.6.1.4.1.14868.3
Az időbélyeg kiadásának UTC időpontja, amely lekövethető a BIPM[62] által kiadott idővel		YYYYMMDDhhmmss[.ss]Z
Pontosság *Accuracy*		Az időmegadás pontosságának értéke. Megadása kötelező.
Rendezés *Ordering*		TRUE
Időbélyeg kérelemben szereplő véletlen szám (nonce) hossza		Ugyanaz, mint amely a időbélyeg kérésben volt.
Időbélyeg kérelemben engedélyezett hash algoritmus		SHA-1
Időbélyeg kérelemben kérhető-e a szolgáltató tanúsítványa (certReq)		Igen
Az időbélyeg válasz aláírásánál használt hash algoritmus		SHA1
Az időbélyeg válasz aláírásánál használt aláíró algoritmus		RSA
Az időbélyeg válasz időfelbontása (genTime)		0,01 másodperc
Időbélyegző szolgáltatás "UTC max offset" értéke		0,1 másodperc
Támogatott elérési protokoll		HTTPS tanúsítvány alapú kliens azonosítással
Sorszám: az időbélyegzőben használt sorszám egyedi a Szolgáltatóra nézve.	Sorszám mérete	Dinamikus hosszúságú.
	Sorszám egyedisége	Nem folytonos, de mindig növekvő érték. Az egyediségnek meg kell maradnia a szolgáltatás lehetséges megszakadása után is.

[62] Bureau International des Poids et Mesures

8. HSzSz adminisztráció

8.1. HSzSz változatkezelési eljárások

8.1.1. HSzSz változtatási eljárások

A Szolgáltató szervezetén belül Hitelesítési Politika és Szabályozási Csoport működik, amely a HSzSz karbantartásáért felelős. A változtatási igényeket e csoport gyűjti, a módosításokat elvégzi, a belső és külső tájékoztatási kötelezettségeknek eleget tesz, s a változtatásokat életbe lépteti.

A változtatásokat gyűjtve a Hitelesítési Politika és Szabályozási Csoport belső nem nyilvános munkaváltozatokat hoz létre a szabályzatokból, melyek a közzététel előtt belső felülvizsgálaton esnek át. A Szolgáltató a változásokat kötegelve szerkeszti új szabályzati változattá, törekedve arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.

A HSzSz módosított változatai mindig új verziószámmal kerülnek nyilvánosságra.

8.1.2. Értesítés nélkül változtatható elemek

A Szolgáltató fenntartja a jogot, hogy a szabályzat nem lényegi elemeit előzetes értesítés és bejelentés nélkül változtassa. Ilyenek lehetnek a helyesírási hibák, formai változtatások, különböző kontaktadatok (web címek, telefonszámok), és egyéb olyan elemek, melyek a tanúsítványok és az időbélyegek biztonsági szintjét, felhasználhatóságát a legkisebb mértékben sem módosítják.

8.1.3. Értesítéssel változtatható elemek

Minden a tanúsítványok biztonsági szintjét, felhasználhatóságát a módosító változtatás értesítésköteles a 8.2 fejezet szerint.

8.1.4. Észrevételek kezelése

A 8.2 fejezet szerint közzétett új HSzSz-el kapcsolatos észrevételeket szolgáltató a hatályba lépést megelőző 14 napig fogadja az ica@mavinformatika.hu e-mail címen. A HSzSz észre-

vételekkel módosított változatát szolgáltató a hatályba lépést megelőző 7. nap zárja le és teszi közzé.

8.1.5. Szabályzati objektumazonosítót vagy mutatót változtató módosítások

Minden olyan jelentősebb módosítás, melyet a Szolgáltató csak az újonnan kibocsátásra kerülő tanúsítványok esetében alkalmaz (s a már kibocsátottak esetében nem) a HSzSz verziószámának fő jegyét, s a szabályzat objektumazonosítóját is módosítja.
E szabályzatok az előző főbb verziótól eltérő web címen kerülnek közzétételre, így csak az újonnan kibocsátott tanúsítványok mutatói fognak rá hivatkozni.

8.2. Közzétételi és tájékoztatási elvek

8.2.1. A HSzSz-ben nem tárgyalt elemek

A Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatások biztonságát nem veszélyezteti. A Szolgáltató több belső biztonsági és egyéb szabályzattal, operatív szintű előírással rendelkezik, melyeket bizalmasan kezel (jelen HSzSz több ilyet is megemlít). A 2.7 pontban leírt tanúsítási eljárások ezeket a dokumentumokat is vizsgálják.

8.2.2. A HSzSz közzététele

A Szolgáltató szabályzatainak a változásokkal egybeszerkesztett új verzióját, annak hatályba lépését megelőzően 30 nappal közzéteszi web oldalán, a http://www.mavinformatika.hu/CA/ címen keresztül. Szolgáltató alkalmanként ezt megelőzően is tájékoztatja a közösséget a tervezett változtatásairól.

8.3. HSzSz elfogadási eljárások

A jelen HSzSz az RFC 2527 szabványnak való megfelelőségét közzététel előtt a Szolgáltató megvizsgálta. A vizsgálatot a Szolgáltató, illetve a külső auditor is elvégzi a 3. táblázatban megadott rendszerességgel.

A szabályzat törvényeknek való megfelelőségét a Hírközlési Felügyelet is vizsgálja a HSzSz hatálybalépését megelőzően.

A Szolgáltató HSzSz-ét, a változásokkal egybeszerkesztett új verzióját, annak hatályba lépését megelőzően 30 nappal átadja a Hírközlési Felügyelet részére. A Szolgáltató alkalmanként ezt megelőzően is konzultál a Hírközlési Felügyelettel a tervezett változtatásairól. Az új változat tervezeteket a Szolgáltató vezérigazgatója hagyja jóvá.

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,
- 2/2002. (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági 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.
- 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,
- Minősített tanúsítványtípus minták minősített hitelesítés-szolgáltatók számára, 1.0 verzió, Hírközlési Felügyelet
- A minősített tanúsítványtípus mintáknak megfelelő szolgáltatási szabályzat minták, 1.0 verzió, Hírközlési Felügyelet

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
- Tanúsítvány politikák
- Időbélyegzés Szolgáltatási Politika
- Általános Szerződési Feltételek
- Előfizetői Szerződés Minta
- A Trust&Sign szolgáltatás informatikai biztonságpolitikája
- A Trust&Sign szolgáltatás biztonsági szabályzata
- A Trust&Sign szolgáltatás üzletmenet-folytonossági terve
- A Trust&Sign szolgáltatás üzemeltetési kézikönyve

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 2527 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és szolgáltatási szabályzat keretrendszer)
- Internet Közösség RFC 2459 ajánlása, (Internet X.509 Nyilvános kulcsú infrastruktúra – Tanúsítvány és Tanúsítvány visszavonási lista profil),
- Internet Közösség RFC 3039 ajánlása, (Internet X.509 Nyilvános kulcsú infrastruktúra – Minősített tanúsítvány profil),
- Európai Unió ETSI TS 101 456 szabvány (Minősített tanúsítványokat kibocsátó hitelesítés-szolgáltatókra vonatkozó szabályozási követelmények),
- Európai Unió ETSI TS 101 862 szabvány, (Minősített tanúsítvány profil),
- RFC – 3161 (Internet X.509 nyilvános kulcsú infrastruktúra időbélyeg protokoll)
- ETSI TS 102 023 (2003.04) (Időbélyegzés szolgáltatókra vonatkozó követelmények)
- ETSI TS 101 861 szabvány (Időbélyegzés profil)
- ISO 3166
- NIST FIPS PUB 140-1 Level 1-3 (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)
- American Bar Association (ABA),
- PKI Assessment Guidelines (PAG),
- CWA 14167-1, és a CWA 14172-1,-2,-3,-4 CEN Workshop Agreement-ek
- ISO/IEC 15408 1999: Információ technológia - Biztonsági módszerek - Informatikai biztonság értékelési kritériumai (1-3 részek)
- MeH 12. ajánlás,
- ITSEC,
- Common Criteria.

9.2. Meghatározások

Aláírás-létrehozó adat: olyan egyedi adat (jellemzően kriptográfiai magánkulcs), amelyet az aláíró az elektronikus aláírás létrehozásához használ.

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

Aláírás-létrehozó eszköz: olyan hardver, illetve szoftver eszköz, amelynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.

Aláíró: az a természetes személy, akihez az elektronikus aláírás hitelesítés-szolgáltató által közzétett aláírás-ellenőrző adatok jegyzéke szerint az aláírás-ellenőrző adat kapcsolódik.

Biztonságos aláírás-létrehozó eszköz: a 2001. évi XXXV. törvény 1. számú mellékletében foglalt követelményeknek eleget tevő aláírás-létrehozó eszköz.

Biztonsági tisztviselő: a szolgáltatás biztonságáért általánosan felelős személy;

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

Elektronikus aláírás ellenőrzése: az elektronikus dokumentum aláíráskori, illetve ellenőrzéskori tartalmának összevetése, továbbá az aláíró személyének azonosítása a dokumentumon szereplő, illetve a hitelesítés-szolgáltató által közzétett aláírás-ellenőrző adat, valamint a Tanúsítvány felhasználásával.

Elektronikus aláírás felhasználása: elektronikus adat elektronikus aláírással történő ellátása, illetve elektronikus aláírás ellenőrzése.

Elektronikus aláírás hitelesítés-szolgáltató: a 2001. évi XXXV. törvény 6. § (2) bekezdése szerinti tevékenységet végző személy (szervezet).

Elektronikusan történő aláírás: elektronikus aláírás hozzárendelése, illetve logikailag való hozzákapcsolása az elektronikus adathoz.

Elektronikus aláírási termék: olyan szoftver vagy hardver, amely elektronikus aláírással kapcsolatos szolgáltatások nyújtásához, így különösen elektronikus aláírások, illetőleg időbélyegző készítéséhez vagy ellenőrzéséhez használható.

Elektronikus dokumentum: elektronikus eszköz útján értelmezhető adat, amely elektronikus aláírással van ellátva.

Elektronikus irat: olyan elektronikus dokumentum, amelynek funkciója szöveg betűkkel való közlése, és a szövegen kívül az olvasó számára érzékelhetően kizárólag olyan egyéb adatokat foglal magában, melyek a szöveggel szorosan összefüggenek, annak azonosítását (pl. fejléc), illetve könnyebb megértését (pl. ábra) szolgálják.

Elektronikus okirat: olyan elektronikus irat, amely nyilatkozattételt, illetőleg nyilatkozat elfogadását, vagy nyilatkozat kötelezőnek elismerését foglalja magában.

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

1. alkalmas az aláíró azonosítására és egyedülállóan hozzá köthető,
2. olyan eszközzel hozták létre, mely kizárólag az aláíró befolyása alatt áll,
3. a dokumentum tartalmához olyan módon kapcsolódik, hogy minden - az aláírás elhelyezését követően az iraton, illetve dokumentumon tett - módosítás érzékelhető.

Időbélyegző: elektronikus irathoz, illetve dokumentumhoz végérvényesen hozzárendelt, illetőleg az irattal vagy dokumentummal logikailag összekapcsolt igazolás, amely tartalmazza a bélyegzés időpontját, és amely a dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden - az igazolás kiadását követő - módosítás érzékelhető.

Igénylő: a minősített tanúsítvány iránti igényt benyújtó személy;

Informatikai rendszer: a szolgáltató által a szolgáltatói kulcspár kezeléséhez, az aláírás-létrehozó adat előállításához, a tanúsítványok kibocsátásához, a kibocsátott Tanúsítványt tartalmazó nyilvántartáshoz, a visszavonási nyilvántartásokhoz és a visszavonás kezelési szolgáltatáshoz, valamint e tevékenységek informatikai védelméhez használt, a 2001. évi XXXV. törvény. 3. számú mellékletének f) pontja szerinti megbízható rendszerek és termékek;

Kriptográfiai kulcs: olyan kriptográfiai transzformációt vezérlő egyedi jelsorozat, amelynek ismerete a rejtjelezéshez vagy a visszaállításhoz, különösen az elektronikus aláírás előállításához vagy ellenőrzéséhez szükséges;

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

Minősített hitelesítés-szolgáltató: a 2001. évi XXXV. törvény 8. § (3) bekezdése szerint nyilvántartásba vett hitelesítés szolgáltató.

Minősített tanúsítvány: a 2001. évi XXXV. törvény 2. számú mellékletében foglalt követelményeknek megfelelő olyan Tanúsítvány, amelyet minősített szolgáltató bocsátott ki.

Rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását a regisztráció, a tanúsítványok előállítása, az aláírás-létrehozó eszközök szolgáltatása és a tanúsítványok visszavonása, felfüggesztése céljából végző személy;

Rendszerüzemeltető: az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy;

Rendszervizsgáló: a szolgáltató naplózott, illetve archivált adatállományát kezelő személy;

Rendkívüli üzemeltetési helyzet: olyan, a szolgáltató üzemmenetében zavart okozó rendkívüli helyzet, amikor a szolgáltató rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincsen lehetőség;

Szolgáltatási szabályzat: a 2001. évi XXXV. törvény 6. § (1) bekezdése szerinti szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat.

Szolgáltatói kulcspár: a szolgáltatói magánkulcs és a szolgáltatói nyilvános kulcs;

Szolgáltatói magánkulcs: olyan kriptográfiai magánkulcs, amelyet a hitelesítés-szolgáltató vagy az időbélyegzést nyújtó szolgáltató saját elektronikus aláírási szolgáltatásának igazolására, így különösen a Tanúsítvány kibocsátására, a visszavonási nyilvántartásokra, az időbélyegzésre, a naplózáshoz, az archiváláshoz használ;

Szolgáltatói nyilvános kulcs: olyan kriptográfiai nyilvános kulcs, amelyet a szolgáltatói magánkulcs használatával létrehozott elektronikus aláírás ellenőrzésére használnak;

Tanúsítvány: hitelesítés-szolgáltató által kibocsátott igazolás, amely az aláírásellenőrző adatot a 2001. évi XXXV. törvény 9. § (3), illetőleg (4) bekezdése szerint egy meghatározott személyhez kapcsolja, és igazolja e személy személyazonosságát.

Tanúsítvány kibocsátása: a Tanúsítvány átadása az aláírónak, valamint a szolgáltató nyilvántartásában a Tanúsítvány elérhetővé tétele az aláíró által meghatározott kör részére;

Visszavonás kezelése: a 2001. évi XXXV. törvény 14. §-ban meghatározott esetekben a kibocsátott tanúsítványok visszavonására és felfüggesztésére vonatkozó eljárások lefolytatása;

Visszavonási nyilvántartások: nyilvántartások a felfüggesztett, illetőleg a visszavont tanúsítványokról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját.