MÁV INFORMATIKA

Kereskedelmi, Szolgáltató és Tanácsadó Kft.

Trust&Sign

Hitelesítés Szolgáltatási Szabályzat
Titkosítás Hitelesítés Szolgáltatáshoz

Verziószám	**1.0**
Hatálybalépés dátuma	**2004. augusztus 1.**

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

A dokumentum neve	Hitelesítés Szolgáltatási Szabályzat Titkosítás Hitelesítés Szolgáltatáshoz (HSzSz)*
HSzSz verziószám	1.0
Üzemelő PKI szoftver verziószám (Technikai azonosító)	Trust&Sign SecureCA v1.0
HSzSz objektum azonosító (OID)	1.3.6.1.4.1.14868.1.3
Első hatálybalépés időpontja	2004. augusztus 1.
Aktuális változat hatálybaléptetés időpontja	2004. augusztus 1.
Következő felülvizsgálat időpontja:	2005. augusztus 31.

* A **MÁV INFORMATIKA Kft.** Hitelesítés Szolgáltatási Szabályzata az elektronikus aláírásról szóló 2001. évi XXXV. törvény szerint előírt Szolgáltatási Szabályzat, 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.

TARTALOMJEGYZÉK

1. Bevezetés

E dokumentum a MÁV INFORMATIKA Kft. (továbbiakban Szolgáltató) Titkosító tanúsítvány-hitelesítés szolgáltatásra vonatkozó, a Titkosító Tanúsítványokra érvényes Hitelesítés Politikában (továbbiakban: HP) meghatározott követelmények szerint a Szolgáltatónál megvalósított eljárásrendet és az egyéb működési szabályokat tartalmazza.

A Szolgáltató a Titkosító tanúsítvány-hitelesítés szolgáltatást a vele előfizetői szerződéses viszonyban álló igénybevevők részére szolgáltatja.

A Szolgáltató a vele szerződéses kapcsolatban álló Titkosító magánkulcs felhasználók részére a következő szolgáltatásokat nyújtja:

- Titkosító kulcspár előállítás,
- Titkosító tanúsítvány hitelesítés,
- Titkosító kulcspár és Tanúsítvány adathordozóra történő elhelyezése,
- Titkosító kulcspár és Tanúsítvány érvényesség kezelés (CRL),
- Titkosító kulcspár és Tanúsítvány biztonságos megőrzése hosszabb távra,
- Titkosító kulcspár visszaállítás a Kulcshordozó elvesztése, illetéktelen kezekbe kerülése esetén.

A HSzSz további fejezeteiben a „*szolgáltatások*” kifejezés alatt a fenti részszolgáltatások bármelyike értendő.

A szolgáltatások részletezése az 1.3.6.2 pontban olvasható.

Ezen szolgáltatásokat a Szolgáltató fokozott biztonságú szinten szolgáltatja.

A jelen Hitelesítés Szolgáltatási Szabályzat (továbbiakban: HSzSz) 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 SecureCA v1.0, röviden: **Trust&Sign SCA 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 Szolgáltató titkosítás-hitelesítés szolgáltatásával valamilyen módon kapcsolatba kerülő feleknek tudni kell vagy érdemes. Biztosítja a Szolgáltató működésének átláthatóságát, s lehetővé teszi a felhasználók és az érintett felek 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 elfogadóinak egyértelműen meg kell tudni állapítani a Tanúsítvány kezelésének módját, az általa garantált hitelesség és biztonság mértékét és az erre vonatkozó technikai, üzleti és pénzügy garanciákat, jogi felelősség vállalásokat.

A tanúsítványok végfelhasználóinak tevékenységére vonatkozóan jelen HSzSz-től és Szolgáltatótól független egyéb 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 jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 1.1.2 fejezetének tartalma érvényes.

1.1.3 Jogszabályok, szabványok

- RFC 2527 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és szolgáltatási szabályzat keretrendszer)
- ISO/IEC 15408 1999: Információ technológia - Biztonsági módszerek - Informatikai biztonság értékelési kritériumai (1-3 részek)
- Európai Unió ETSI TS 101 456 szabvány,
- ITU-T X.509 “Information technology - Open Systems Interconnection - The Directory: Public -key and attribute certificate frameworks” ajánlás 3. verziója,
- RFC 2459 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítvány és tanúsítvány visszavonási lista profil)

- MeH 12. ajánlás, ITSEC[1], CC[2]
- NIST FIPS PUB 140-1 (1994. január 11.) (Kriptográfiai modulok biztonsági követelményei),
- CWA 14167-1, és a CWA 14172-1,-2,-3,-4 CEN Workshop Agreement-ek

1.2 HSzSz azonosítás

Az elektronikus aláírásról szóló évi XXXV. törvény 7. § 1. bekezdés értelmében a Szolgáltató tevékenységének megkezdése előtt 30 nappal bejelentette fokozott biztonságú aláírás-hitelesítés szolgáltatási szándékát a Nemzeti Hírközlési Hatóságnak a törvény által előírt dokumentumok kíséretében. A Hatóság a fokozott biztonságú elektronikus aláírás hitelesítés szolgáltatási tevékenység folytatására az engedélyt megadta, és a Szolgáltatót nyilvántartja (nyilvántartási adatokat ld. 1.5 pont). A Szolgáltató a Titkosító tanúsítvány-hitelesítés szolgáltatását ezen engedélyezett tevékenység keretében a fokozott biztonsági szintnek megfelelően nyújtja.

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

Jelen dokumentum teljes neve: **Trust&Sign Hitelesítés Szolgáltatási Szabályzat Titkosítás Hitelesítés Szolgáltatáshoz.** A jelen dokumentumban HSzSz-ként történik rá hivatkozás.

A titkosító tanúsítványokra érvényes Policy OID: 1.3.6.1.4.1.14868.2.3

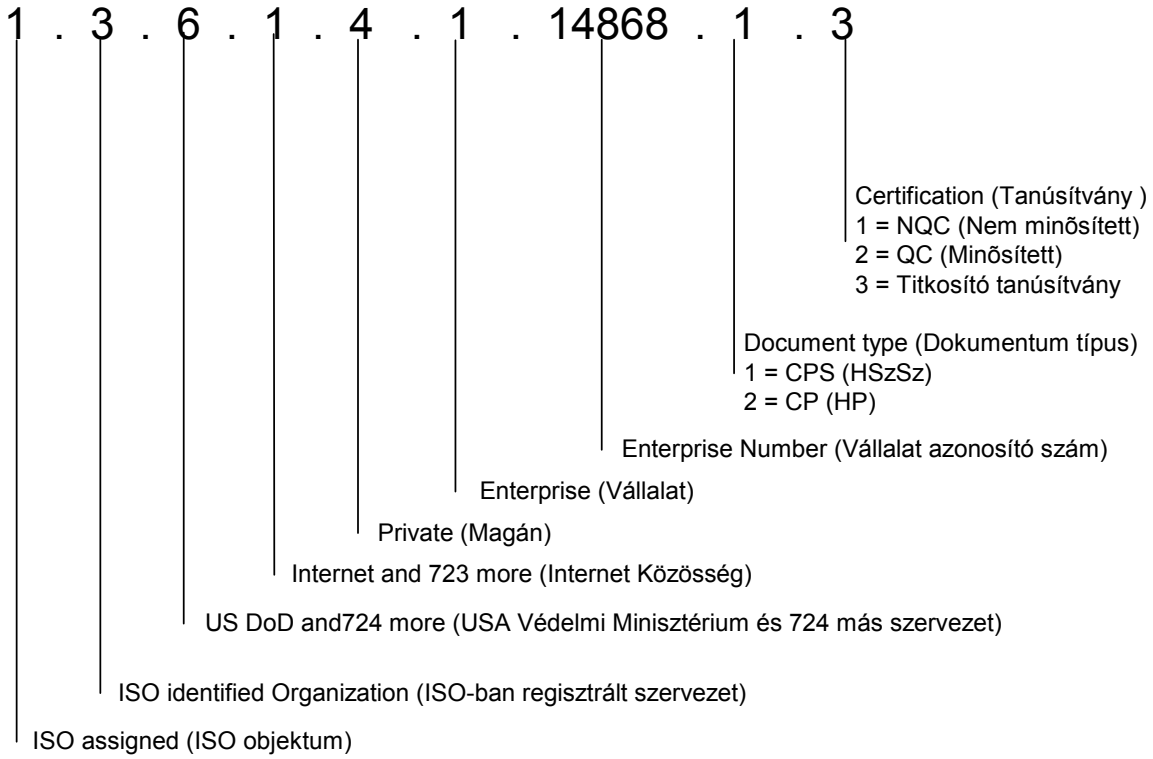
A jelen HSzSz Interneten a következő címen érhető el: *http://www.mavinformatika.hu/ca.*

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

[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.

OID szám:



1. ábra

1.3 Hitelesítés szolgáltató és felhasználó közösség, alkalmazhatóság

A Szolgáltató által kibocsátott tanúsítványokat felhasználó közösség a következő:

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

1.3.1 Hitelesítési Politika és Szabályozási Csoport

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 1.3.1 fejezetének tartalma érvényes.

1.3.2 Hitelesítő Központ ("CA")

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 1.3.2 fejezetének tartalma érvényes.

1.3.3 Regisztrációs Iroda ("RA")

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

- Regisztrációs Iroda (rövidítve: RA),
- Ügyfélkapcsolati Irodák (rövidítve: ÜKI), 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 a Kulcshordozó eszközön a Titkosító magánkulcs elhelyezését. Egyúttal közreműködik a titkosítással kapcsolatos további szolgáltatások biztosításában: Tanúsítvány előállítás, Tanúsítvány kibocsátás és visszavonási állapot közzététele.

A Regisztrációs Irodához kapcsolódó feladat-, felelősség- és hatásköröket a PKI Üzleti Egység gyakorolja.

1.3.4 Ügyfélkapcsolati Irodák ("ÜKI")

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 1.3.4 fejezetének tartalma érvényes.

1.3.5 Felhasználók

1.3.5.1 Előfizető

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

Az Előfizető egyben Titkosító magánkulcs felhasználó is, amennyiben saját maga képviseletében a titkosítási jogosultsággal is rendelkezik, azaz birtokolja és használja a Titkosító magánkulcsot.

Az Előfizető lehet jogi személy (szervezet) is. Ebben az esetben a szervezet képviselőként egy természetes személyt bíz meg, akit felruház hagyományos, illetve elektronikus aláírási jogosultsággal, valamint rendelkezik a 6.1.2 pontban meghatározott transzport magánkulccsal. Ez a személy a jogi személyt képviselve ír alá hagyományos papíralapú, illetve elektronikus dokumentumokat.

Titkosító magánkulcs felhasználó lehet:

a) bármely természetes személy, aki személyazonosságát a regisztráció során az általa igényelt tanúsítvány osztálynak megfelelően, a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz 3.1.8 és 3.1.9 pontjaiban előírtak szerint igazolta.

b) bármely természetes személy, aki részére a Tanúsítvány azzal a céllal kerül kibocsátásra, hogy a Titkosító magánkulcs felhasználót más természetes vagy jogi személy (szervezet) képviseletében történő titkosított adatállomány visszaállítására jogosítsa fel. Ebben az esetben a Titkosító magánkulcs felhasználó személyazonosságának ellenőrzése mellett a regisztráció során a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz 3.1.8 és 3.1.9 pontjaiban meghatározott módon a képviseleti jogosultságot is ellenőrizni kell.

1.3.5.2 Érintett fél

Az Érintett fél olyan természetes személy, aki saját maga vagy az őt alkalmazó jogi személy képviseletében a Titkosító magánkulcs felhasználónak elküldendő állományt annak Nyilvános kulcsával titkosítja.

Az Érintett fél ezen műveletnél a Titkosító magánkulcs felhasználó Nyilvános kulcsához tartozó Tanúsítvány érvényességi ellenőrzésére hagyatkozva jár el.

1.3.6 Alkalmazhatóság

1.3.6.1 Szabályzat hatálya

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 1.3.6.1 fejezetének tartalma érvényes.

1.3.6.2 Szolgáltatás szintje

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

- Regisztráló szolgáltatás
- Egyedi-név szolgáltatás
- Titkosító kulcspár létrehozási szolgáltatás

- Tanúsítvány létrehozási szolgáltatás
- Tanúsítvány szétosztási (publikálási) szolgáltatás
- Tanúsítvány visszavonás kezelési szolgáltatás
- Titkosító magánkulcs elhelyezés Kulcshordozó eszközön
- Kulcshordozó eszköz fizikai megszemélyesítése (szolgáltató arculati elemeinek elhelyezése az eszközön)
- Kulcshordozó eszköz logikai megszemélyesítése (Tanúsítványok és magánkulcs elhelyezése a hordozó eszközön)
- Titkosító magánkulcs biztonságos tárolása szolgáltatás
- Titkosító magánkulcs visszaállítás a tárolt példány alapján
- Tanúsítvány archiválási szolgáltatás
- Állapotinformációs szolgáltatás
- Adattárolási szolgáltatás
- Tanúsítvány megújítási szolgáltatás;

A Szolgáltatások megfelelőségét külső auditor tanúsítja.

1.3.6.3 Tanúsítványok alkalmazhatósága

A tanúsítványok alkalmazhatóságára a következő alapszabályok érvényesek:

1. Engedélyezett alkalmazási lehetőségek

   A kibocsátott nyilvános kulcs csak elektronikus állományok titkosítására, a magánkulcs pedig csak a titkosított elektronikus állományok visszaállítására használható fel, a Tanúsítványba foglaltaknak megfelelően.

2. Korlátozott alkalmazási lehetőségek

   Szolgáltató területi, pénzügyi, stb. korlátozásokat szabhat saját belső hitelesítési politikája (HP) szerint, amelyeket a kibocsátott előfizetői Tanúsítványban megad.

   Egyébként a Szolgáltató csak annyiban korlátozza a kibocsátott Tanúsítvány felhasználhatóságát, hogy a hozzátartozó kulcspár csak az előző (1.3.6.3 fejezet 1.) pont szerinti célra használható. Az Előfizető szervezet élhet korlátozásokkal a Titkosító magánkulcs felhasználó és az érintett felek Tanúsítvány felhasználási tevékenységével kapcsolatosan.

3. Tiltott alkalmazási lehetőségek

Az előfizetői tanúsítványok más nyilvános kulcsú tanúsítványok aláírására történő felhasználása, vagy bármilyen hitelesítés szolgáltatás nyújtásához történő alkalmazása tilos.

A fentiek alapján a kibocsátott tanúsítványok (illetve az ezekhez kapcsolódó kulcspárok) felhasználhatók minden olyan számítástechnikai alkalmazásban, amelyek támogatják a PKI technológián alapuló titkosítási funkciókat. Amennyiben a Szolgáltató titkosítás céljából bocsát ki Tanúsítványt, a Tanúsítványhoz kapcsolódó magán-, illetve nyilvános kulcsot kizárólag titkosításra lehet felhasználni.

A Szolgáltató nem vállal felelősséget a titkosításra kibocsátott Tanúsítvány, illetve az ehhez kapcsolódó kulcspárok titkosítástól eltérő felhasználásáért.

Jelen HSzSz hatálya alatt kibocsátott tanúsítványok csak az 1.3 fejezetben meghatározott hitelesítés-szolgáltató és felhasználó közösség körében használhatók az Általános Szerződési Feltételek Fokozott Biztonságú Hitelesítés Szolgáltatáshoz c. dokumentumban (továbbiakban: ÁSzF), illetve az Előfizetői Szerződésben meghatározott összeghatárok szerinti korlátokkal.

A Tanúsítvány használati lehetőségére vonatkozó fenti információk a Tanúsítványban is rögzítésre kerülnek. A Tanúsítvány elfogadása, a feltüntetett használati információktól eltérő bármely módú használata a Titkosító magánkulcs felhasználó és az Érintett fél egyéni felelőssége és kockázata.

A titkosításra kibocsátott kulcsok és Tanúsítványok kizárólag titkosított állomány létrehozására, illetve annak visszaállítására használhatók. A Szolgáltató nem vállal felelősséget a titkosításra kibocsátott kulcsok és Tanúsítványok titkosítástól eltérő célú használatáért.

1.4 Tanúsítványok típusa, tanúsítvány osztály és tanúsítvány fajta

A jelen HSzSz csak a nem minősített (NQC[3]) - azaz fokozott biztonságú aláíró tanúsítvánnyal azonos biztonsági szintű - és nyilvános körben kibocsátott titkosító tanúsítványokat és az ezzel kapcsolatos szabályokat írja le.

A jelen HSzSz hitelességi szint szempontjából csak a titkosító tanúsítványok osztályát ismerteti, a titkosító teszt tanúsítványokkal nem foglalkozik.

A jelen HSzSz a tanúsítványok felhasználási területe és célja szerint a következő tanúsítvány fajtákat különbözteti meg:

- Előfizetői tanúsítványok
- Szolgáltatói tanúsítványok

A Szolgáltató felelősségvállalása egyszintű.

Felelősségvállalással Tanúsítvány értelemszerűen csak az Előfizetőnek adható ki.

A felelősségvállalás mértékét az Előfizetői Szerződés rögzíti, a számszerűsített felelősségvállalást a kibocsátott Tanúsítványban is szerepeltetni kell.

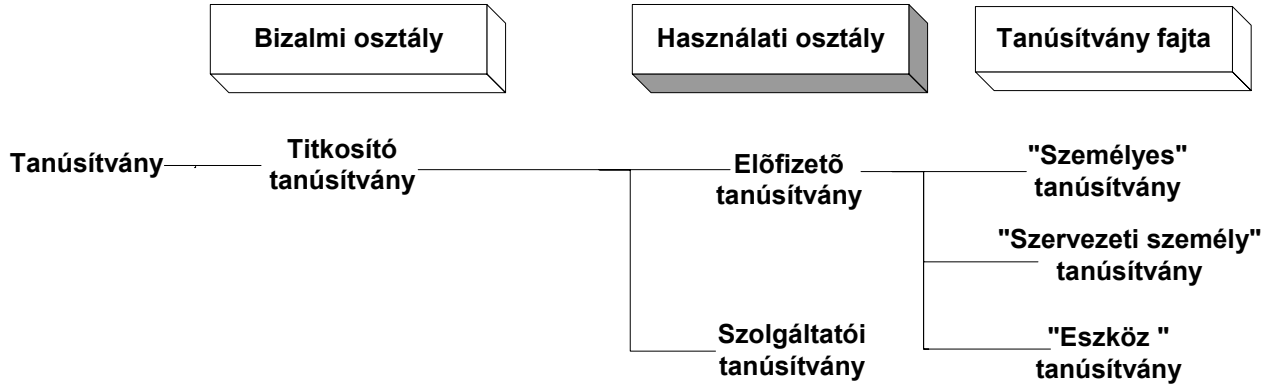
A jelen HSzSz a következő tanúsítvány típusokat különbözteti meg:

- személyes típusú tanúsítvány,
- szervezeti személy típusú tanúsítvány,
- eszköz tanúsítvány.

A Szolgáltató a jelen HSzSz által meghatározott szolgáltatási körében csak titkosító tanúsítványokat bocsát ki.

A 2. ábra mutatja a Titkosító tanúsítvány osztály szerkezetét.

[3] A CWA 14167-1:2001 (E) szerint meghatározott nem minősített tanúsítványok, angolul: Non Qualified Certificate (NQC)



2. ábra

A következő pontokban megadjuk az egyes Tanúsítvány osztályok és fajták meghatározását.

1.4.1 Tanúsítványok osztályai, fajtái és tulajdonságaik

1.4.1.1 Nem minősített Tanúsítvány

A Szolgáltató által kibocsátott Titkosító tanúsítvány:

- amelynek „kulcsfelhasználás” mezejében a tikosításra utaló paraméter van megjelölve,
- fokozott biztonsági szinttel azonos biztonsági szintű,
- csak titkosítás céljára használható,
- államtitok vagy szolgálati titok szinten minősített adatokat tartalmazó állomány titkosítására nem használható.

1.4.1.2 Teszt tanúsítvány

A Szolgáltató titkosító teszt tanúsítványokat is kibocsáthat. Jelen HSzSz ezen tanúsítványokra nem vonatkozik.

1.4.1.3 Előfizetői Tanúsítvány

Előfizetői Tanúsítvány a Szolgáltatóval az Előfizetői Szerződés által szerződéses viszonyba kerülő Előfizető számára kibocsátott Tanúsítvány, amely csak titkosítási célú lehet. Előfizetői Tanúsítvány csak felelősség vállalással bocsátható ki, amelynek mértékét az Előfizetői Szerződésben kell rögzíteni.

Előfizetői Tanúsítvány olyan természetes személyeknek vagy szervezeteknek kerül kiadásra, amelynél a Titkosító magánkulcs felhasználót 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	A Titkosító magánkulcs felhasználó személyi igazolványának vagy útlevelének bemutatása személyesen. Képviseleti megbízás cégszerűen aláírva.
Szervezet	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.
Eszköz	Természetes személy esetén az azonosított és hitelesített Előfizető írásos nyilatkozata az eszköz birtoklásáról és az eszköz azonosítójáról. Jogi személy esetén a szervezet és a megbízott képviselő azonosítása és hitelesítése után, a képviselőnek át kell adnia egy cégszerű aláírással ellátott nyilatkozatot az eszköz birtoklásáról és az eszköz azonosítójáról.

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 jogi személynek (szervezetnek) írásban kell nyilatkoznia arról is, hogy a Titkosító magánkulcs felhasználó hiteles személyazonosságának megállapítása a szervezeten belül már előzetesen megtörtént.

A Szolgáltató a megbízott képviselő személyt nyilvántartja és bármely, a képviselt személy (vagy szervezet) nevében történő eljárás esetén a képviselő személy azonosítását-hitelesítését a Titkosító magánkulcs felhasználó, illetve az Előfizető esetében szokásos eljárásnak megfelelően végzi el.

1.4.1.4 Szolgáltatói Tanúsítvány

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

1.4.2 Tanúsítvány fajták és tulajdonságaik

A Szolgáltató a következőkben meghatározott nem minősített titkosító tanúsítványokat adhatja ki előfizetők részére, illetve saját céljaira.

1.4.2.1 „Személyes" típusú tanúsítvány

Személyes típusú tanúsítványokat természetes személy igényelhet a saját nevében. A személyes típusú tanúsítvány esetében az Előfizető és a Titkosító magánkulcs felhasználó ugyanaz a személy.

A személyes típusú tanúsítvány igénylésekor az Ügyfélkapcsolati Irodán történő azonosítás-hitelesítésnél a következő adatokat kell kezelni:

- a Titkosító magánkulcs felhasználó neve, aláírása,
- a Titkosító magánkulcs felhasználó okmányszáma (személyi igazolvány vagy útlevél szám),
- a Titkosító magánkulcs felhasználó lakcíme,
- a Titkosító magánkulcs felhasználó e-mail címe.

A Tanúsítvány „Country" és „Locality" mezőjében az Igénylő lakóhelyének országkódja és helységneve, az „E" mezőben az Igénylő e-mail címe, a „Common Name" mezőben az igénylő neve szerepel. A Tanúsítvány „Organization" és „Organization Unit" mezői üresen maradnak.

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

1.4.2.2 „Szervezeti személy" típusú tanúsítvány

„Szervezeti személy" típusú tanúsítványokat természetes személy igényelhet egy adott szervezet alkalmazottjaként és/vagy tisztségviselőjeként. A szervezet - többek között - lehet gazdálkodó szervezet, hivatal, önkormányzat, egyesület, alapítvány, stb.

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

A „Szervezeti személy" típusú tanúsítványok igénylésekor 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 és 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,
- Titkosító magánkulcs felhasználására kijelölt személy beosztása,
- Titkosító magánkulcs felhasználására kijelölt személy személyi igazolvány vagy útlevél száma,
- Titkosító magánkulcs felhasználására kijelölt személy telefon száma, e-mail címe.

A fentieken kívül még a következőket kell megadni:

- Titkosító magánkulcs felhasználására 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 (un. Kapcsolattartó) 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 szervezete telephelyének országkódja és városa, az „Organization” mezőben a szervezetének neve, az „Organizational Unit” mezőben az igényt támasztó szervezeti egység neve, az „E” mezőben a szervezeti személy e-mail címe, a „Common Name” mezőjen a szervezeti személy neve szerepel.

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

1.4.2.3 Eszköz tanúsítvány

Eszköz tanúsítványt természetes személy vagy szervezet igényelhet az általa működtetett IP címmel rendelkező informatikai eszköz részére. Tipikus eszközök: web szerver, WAP szerver, VPN, stb. Eszköz tanúsítványigénylésnél Előfizetőnek az a természetes vagy jogi személy számít, akivel/amellyel a szerződés megkötésre került.

Az Ügyfélkapcsolati Irodán történő azonosítás-hitelesítésnél a következő adatokat kell megadni:

- az igénylő személy/szervezet neve, lakhelye/székhelye,
- annak a személynek/szervezeti egységnek a neve, telefon és fax száma és e-mail címe, amely az eszközt üzemelteti,

- az eszköz azonosítója, pl. web szerver esetén a szerver internetes, ún. host neve.

A Tanúsítvány „Country” és „Locality” mezőjében a szervezet telephelyének országkódja és városa, az „Organization” mezőben a szervezet neve, az „Organizational Unit” mezőben a szervezeti egység neve, a „Common Name” mezőjében ismételten az „Organization” és az „Organizational Unit” értékek szerepelnek.

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/ca*

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 Hitelesítési 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 politikákban, az ÁSzF-ben, az Előfizetői Szerződésekben és a Biztonsági Szabályzatban meghatározottak szerint jár el az előfizetők tanúsítványainak kiadásakor és kezelésekor, amelynek keretében kötelezettséget vállal az alábbiakra:

1. A Szolgáltató (a Hitelesítő Központ, a Regisztrációs Iroda, az Ügyfélkapcsolati Irodák és az Ügyfélszolgálat együttes tevékenységével) az 1. és az 1.3.6.2. pontokban megjelölt szolgáltatásokat biztosítja. A szolgáltatások megnevezése: Trust&Sign szolgáltatások.
2. A Szolgáltató gondoskodik a Szolgáltatóra és a szolgáltatásra vonatkozó valamennyi, a jelen HSzSz-ben részletezett állítás teljesüléséről, amennyiben azok az adott tanúsítványtípusra alkalmazhatók.
3. A Szolgáltató jogi személy.
4. A Szolgáltató megfelelően dokumentált megállapodásokkal és szerződéses kapcsolatokkal rendelkezik azon esetekre, amikor a szolgáltatások nyújtása alvállalkozókat, illetve más, harmadik felekkel kötött megegyezéseket érint.
5. A Szolgáltató az 1. pontban megjelölt szolgáltatásait a HSzSz szerint nyújtja.
6. A HSzSz-t a Szolgáltató vezetése hagyja jóvá; a HSzSz megfelelő megvalósításáért a Szolgáltató vezetése felel.
7. A Szolgáltató rendszeresen felülvizsgálja HSzSz-ét, az újra érvényesített szabályzat tartalmazza a szükséges módosításokat.
8. A Szolgáltató a fenti (a 7. pont szerint történő) jóváhagyást követően az átdolgozott szolgáltatási szabályzatát (ezen felsorolás 15. pontjában előírtak szerint) a hatálybalépés napjától hozzáférhetővé teszi.
9. A Szolgáltató mindenkor a Titkosító magánkulcs felhasználó által szolgáltatott, az Ügyfélkapcsolati Irodák által a HSzSz-ben és Előfizetői Szerződésben meghatározott módon jóváhagyott adatok alapján bocsátja ki a Tanúsítványt.
10. A Szolgáltató a Tanúsítvány kibocsátását követően a Tanúsítvány azonosító adataiban változást nem eszközölhet. Az Előfizető, illetve a Titkosító magánkulcs felhasználó által – a Tanúsít-

ványban foglalt adatok változására vonatkozó – bejelentés automatikusan a Tanúsítvány visszavonását vonja maga után. A módosított adatokkal kibocsátott Tanúsítvány új Tanúsítványnak minősül.

11. 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.
12. 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 feldolgozásáról intézkedik és a Tanúsítvány kibocsátásáról az Előfizetőt az Ügyfélkapcsolati Iroda útján 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 Irodák részére.
13. A Szolgáltató a szolgáltatások működtetése és menedzselése során a HSzSz-ben, az ÁSzF-ben, illetve az Előfizetői Szerződésben rögzített ügyfélkapcsolati tevékenységet az Ügyfélkapcsolati Irodák által biztosítja, amely fogadja az igénylőket, megadja a szükséges tájékoztatást és információkat, szerződést köt, átadja a Kulcshordozó 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.
14. A Szolgáltató vezeti és közzéteszi a jogszabály szerinti nyilvántartásokat, valamint a Tanúsítvány kibocsátására vonatkozó saját szabályzatait (HSzSz, ÁSzF), Internet segítségével bárki számára elérhető módon.
15. A Szolgáltató értesítést küld e-mail-ben a lejáró Tanúsítványokról az Előfizető és a Titkosító magánkulcs felhasználó részére legalább 15 nappal a lejárat előtt, és kéri az Előfizető, illetve a Titkosító magánkulcs felhasználó további intézkedését a tanúsítvánnyal kapcsolatban. Az e-mail értesítés felhívja az Előfizető és a Titkosító magánkulcs felhasználó figyelmét arra, hogy a Tanúsítvány lejáratát követően azt nem használhatja. Amennyiben az Előfizető, illetve a Titkosító magánkulcs felhasználó 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.

16. Szolgáltató a Tanúsítvány megfelelő mezőjében feltünteti, ha az ÁSzF, illetve az Előfizetői Szerződés a Tanúsítvány felhasználhatóságával kapcsolatban összeg, területi vagy egyéb korlátozásokat tartalmaz.
17. A Szolgáltató felfüggeszti a Tanúsítvány érvényességét és ezt nyilvánosan elérhető helyen közzéteszi (a *http://www.mavinformatika.hu/ca* web lapon keresztül), amennyiben:
    17.1. az Előfizető vagy a Titkosító magánkulcs felhasználó ezt az ÁSzF-ben meghatározott módon kéri,
    17.2. a szolgáltatásokkal kapcsolatos – jogszabályban meghatározott – rendellenességről szerez tudomást,
    17.3. megalapozottan feltételezhető, hogy a Tanúsítványban foglalt adatok nem felelnek meg a valóságnak, vagy a Titkosító magánkulcs nem a Felhasználó kizárólagos birtokában van,
    17.4. a Nemzeti Hírközlési Hatóság jogerős és végrehajtható határozatában így rendelkezik.
18. A Szolgáltató köteles a Tanúsítvány visszavonására és ennek közzétételére az alábbi esetekben:
    18.1. amennyiben ezt a Titkosító magánkulcs felhasználó, szervezeti személy típusú Tanúsítvány esetén az általa képviselt jogi személy a mindenkori HSzSz-ben, illetve az ÁSzF-ben meghatározott módon kéri,
    18.2. amennyiben a képviseleti jogosultság megszűnéséről a képviselt természetes vagy jogi személy illetve a képviselő a Szolgáltatónak bejelentést tesz,
    18.3. amennyiben a Szolgáltató a szolgáltatással kapcsolatos – a HSzSz-ben meghatározott – rendellenességről vesz tudomást és a rendellenesség az ezen dokumentumokban meghatározott szabályok szerint nem orvosolható,
    18.4. amennyiben tudomására jut, hogy a Tanúsítványban foglalt adatok nem felelnek meg a valóságnak, vagy a Titkosító magánkulcs nem a Titkosító magánkulcs felhasználó kizárólagos birtokában van,
    18.5. a Szolgáltató és az Előfizető között a szerződés megszűnt,
    18.6. a Hatóság jogerős és végrehajtható határozatában így rendelkezik,
    18.7. a Szolgáltató a tevékenységét befejezte,
19. 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.
20. A Tanúsítványok lejárat előtti visszavonásának jogkövetkezményei az alábbiak:
    20.1. a visszavont Tanúsítvány a továbbiakban a jelen HSzSz 1.3.6.3 pontjában meghatározott tevékenységek végzésére nem használható.

20.2. a visszavonást követően nem kerül automatikusan új Tanúsítvány kibocsátásra; azt az új Tanúsítványok igénylésével azonos igénylési folyamatnak kell megelőznie.

21. Szolgáltató megőrzi a Tanúsítványokkal kapcsolatos elektronikus információkat és az ahhoz kapcsolódó személyes adatokat legalább a Tanúsítvány érvényességének lejáratától származó 10 évig, illetőleg – amennyiben ezen időszakban a titkosítással, illetve a titkosított elektronikus dokumentummal kapcsolatosan jogvita merül fel és azt a Szolgáltatónak írásban bejelentették – a jogvita jogerős lezárásáig. Ugyanezen határidőig olyan eszközt is biztosít, mellyel a kibocsátott Tanúsítvány tartalma megállapítható.
22. A Szolgáltató annak érdekében, hogy a Titkosító tanúsítvány visszavonása után is visszaállíthatók legyenek a korábban titkosított állományok, a visszavont tanúsítványokhoz tartozó Titkosító magánkulcsokat olyan biztonságos feltételek mellett tárolja, hogy akár külső, akár belső személyek illetéktelen hozzáférése ne legyen megvalósítható.
23. A Szolgáltató tevékenységi köréből csak az új Tanúsítvány kibocsátást szüneteltetheti. Ha a Szolgáltató be kívánja fejezni tevékenységét, erről a tevékenység befejezését legalább hatvan nappal megelőzően értesítenie kell az Előfizetőket, az általa kibocsátott és még vissza nem vont Tanúsítványok Titkosító magánkulcs felhasználóit, általuk képviselt természetes vagy jogi személyt, a 24. pont szerinti szervezetet. A bejelentés időpontjától kezdve a Szolgáltató nem bocsáthat ki új Tanúsítványt. A Szolgáltató a tevékenység befejezését legalább húsz napot megelőzően köteles az általa kibocsátott, és még vissza nem vont Tanúsítványokat visszavonni. A Szolgáltató a Tanúsítványok visszavonását követően a tevékenysége befejezéséig a nyilvánosságra hozatali kötelezettségének továbbra is köteles eleget tenni.
24. 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.
25. A Szolgáltató az Előfizetői Szerződésben rögzíti a szolgáltatás díjtételeit.

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

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 2.1.2 fejezetének tartalma érvényes.

2.1.3 A Hitelesítési Politika és Szabályozási Csoport feladatai és hatásköre

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 2.1.3 fejezetének tartalma érvényes.

2.1.4 A Regisztrációs Iroda ("RA") feladatai és hatásköre

A Regisztrációs Iroda biztosítja az alábbi, a titkosítás-hitelesítéssel kapcsolatos szolgáltatásokat:

- Titkosítás-hitelesítés szolgáltatás, ezen belül:
  - regisztráció,
  - Tanúsítvány felfüggesztés és visszavonás kezelés,
- Titkosító magánkulcs elhelyezése kulcshordozó eszközön.

Egyúttal közreműködik az alábbi, a titkosítás-hitelesítéssel kapcsolatos szolgáltatások biztosításában:

- Titkosító tanúsítvány előállítás,
- Titkosító tanúsítvány kibocsátás
- visszavonási állapot közzététele
- Titkosító tanúsítvány újrakiadás

A Regisztrációs Iroda a regisztráció szolgáltatás keretén belül:

1. 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;

A Regisztrációs Iroda a Tanúsítvány felfüggesztés és visszavonás kezelés szolgáltatás keretén belül:

1. formai szempontból ellenőrzi a Tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmek hitelességét és érvényességét (lásd még 4.4.2 és 4.4.6), valamint szabályosságát (lásd még 4.4.3 és 4.5.7),
2. haladéktalanul, maximum a 4.4.4 pontban meghatározott időn belül végrehajtja a hiteles, érvényes és szabályos, Tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket (vagyis a kérelmezett változást átvezeti a Tanúsítványtár 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[4], 95,5%-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 a Titkosító magánkulcs elhelyezése kulcshordozó eszközön szolgáltatás keretén belül:

1. gondoskodik valamennyi általa, a Titkosító magánkulcs felhasználó számára végrehajtott kulcs előállítás biztonságosságáról, a Felhasználó magánkulcsának titkosságáról,
2. biztonságos módon eljuttatja a Titkosító magánkulcs felhasználó részére előállított kulcspárt a Kulcshordozó eszközbe, egy, a kriptográfiai eszköz és a Kulcshordozó eszköz közötti olyan biztonságos útvonal kiépítésével, mely megfelelő kriptográfiai mechanizmusok felhasználásával forráshitelesítést, sértetlenséget és bizalmasságot biztosít,
3. gondoskodik az általa megszemélyesített Kulcshordozó eszköznek az Ügyfélkapcsolati Irodához történő biztonságos továbbításáról,
4. ellenőrzi a Kulcshordozó eszköz kezelését,
5. a Kulcshordozó eszköz előkészítését megfelelően biztonságos környezetben hajtja végre,
6. biztonságos módon előállítja a kezdeti aktivizáló adatot (PIN kódot), majd sértetlenül eljuttatja az Ügyfélkapcsolati Irodához,
7. biztosítja, hogy a Szolgáltató alkalmazottai nem élhetnek vissza a Kulcshordozó eszközzel,
8. biztosítja saját magánkulcsainak biztonságos használatát és tárolását.

A Regisztrációs Iroda a Titkosító 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 eljárás szerint,
2. új Titkosító tanúsítvány kérelem esetén a Kulcshordozó eszközön a Titkosító magánkulcs elhelyezése szolgáltatással együttműködve gondoskodik az új kulcspár előállításáról, majd a nyil-

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

vántartásban szereplő adatokból[5] és az újonnan előállított Nyilvános kulcsból összeállítja az aláírandó új Tanúsítványt,

3. feldolgozza a teljes, pontos, hiteles és teljesíthető tanúsítvány megújítási kérelmeket az alábbi módon:
   - a Tanúsítványhoz tartozó kulcscsere kérelem esetén ellenőrzi a már korábban nyilvántartásba vett Titkosító magánkulcs felhasználótól érkező Tanúsítvány megújítási kérelem teljességét, pontosságát, hitelességét és teljesíthetőségét a HSzSz 3.1 pontjában a kezdeti regisztrációnál meghatározott ellenőrzési módszerrel;

     a hitelesség ellenőrzéséhez a Tanúsítvány visszavonása utáni első esetben a Szolgáltató nem követeli meg a Titkosító magánkulcs felhasználó ismételt személyes megjelenését, elfogad, illetve feldolgoz minősített elektronikus aláírással hitelesített elektronikus kérelmet is[6]. A második kulcscsere igénynél a személyes megjelenés is szükséges az azonosítás-hitelesítéshez,
4. a Tanúsítvány kibocsátásához szükséges ellenőrzések és visszaigazolások sikeres befejeződése után a hitelesítő szervezet felé Tanúsítvány kibocsátási kérelem üzenetet indít el,
5. biztosítja az aláírandó Tanúsítványt is tartalmazó Tanúsítvány kérelem üzenet sértetlenségét, hitelességét és bizalmasságát.

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

1. fogadja a Hitelesítő Központtól kapott új tanúsítványokat, valamint ellenőrzi ezek hitelességét és sértetlenségét,

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

1. rendkívüli esetben[7] 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,

[5] Egyúttal a regisztráció szolgáltatással együttműködve ellenőrzi, hogy a tanúsítványtulajdonos azonosságának és jellemzőinek igazolására használt információ érvényes-e még.
[6] Ez nem vonatkozik a tanúsítvány aktualizálásra, ahol a Szolgáltató a Titkosító magánkulcs felhasználó személyes megjelenését követeli meg.
[7] Rendkívüli esetnek számít a Szolgáltató szolgáltatói magánkulcsának kompromittálódása, illetve jelentős számú új tanúsítvány visszavonási kérelem beérkezése.

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 Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz 3.1 pontjában és az ÁSzF-ben előírt adatszolgáltatási követelmények szerint megadott adatok alapján a Tanúsítványt igénylő természetes, illetve jogi személy és képviselője azonosságát és a leendő Titkosító magánkulcs felhasználó azon egyedi jellemzőit, melyet a Tanúsítvány igazol,
3. összegyűjti, illetve meghatározza a Tanúsítványba kerülő adatokat, ellenőrzi az Igénylő által átadott dokumentumok valódiságát, érvényességét, sértetlenségét és hitelességét,
4. összeveti egymással és a valósággal az egyes iratokon szereplő adatokat,
5. amennyiben lehetséges, ellenőrzi a dokumentumok érvényességét, valódiságát valós idejű nyilvántartásokban is,
6. nyilvántartásba vesz minden, a tanúsítványok kiadásához kapcsolódó, 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
8. bizalmas információként kezeli az Előfizető és a Titkosító magánkulcs felhasználó minden adatát, kivéve azokat, amelyeket a 2.8 pont tárgyal. A Szolgáltató a birtokába jutott bizalmas információkat a személyes adatok védelméről szóló 1992 évi LXIII. törvénynek megfelelően kezeli, s csak a 2.8.4 - 2.8.7 pontokban említett esetekben és személyek részére fedi fel őket,

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. visszautasítja (az ok megjelölésével) a nem hiteles, érvénytelen, vagy szabálytalan, tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket,
3. a visszavonási kérelem elfogadása után haladéktalanul, maximum a 4.5.4 pontban meghatározott időn belül intézkedik egy Tanúsítvány visszavonásáról,

4. tájékoztatja a visszavont, illetve felfüggesztett Tanúsítvány tulajdonosát Tanúsítványa állapotának változásáról.

Az Ügyfélkapcsolati Iroda a titkosító magánkulcs elhelyezése szolgáltatás keretén belül:

1. gondoskodik valamennyi általa, a Titkosító magánkulcs felhasználó számára előállított titkosító magánkulcs hordozó eszköz és a PIN kód biztonságos kezeléséről és a Titkosító magánkulcs felhasználónak történő biztonságos átadásukról,
2. biztosítja, hogy a Szolgáltató alkalmazottai nem élhetnek vissza a titkosító magánkulcs hordozó eszközzel.

Az Ügyfélkapcsolati Iroda a Tanúsítvány előállítás szolgáltatásban való közreműködés keretén belül:

1. kezdeti Tanúsítvány előállítás esetén ellenőrzi a regisztráció szolgáltatás 3., 4., és 5. pontjaiban leírt módon összegyűjtött, Tanúsítványba kerülő adatokat az adott tanúsítványtípushoz kapcsolódó hitelesítési, ellenőrzési eljárás szerint,
2. a Titkosító magánkulcs felhasználó adatainak változása, illetve kulcscsere kérelem esetén ellenőrzi a már korábban nyilvántartásba vett Titkosító magánkulcs felhasználótól érkező Tanúsítvány megújítási kérelem teljességét, pontosságát, hitelességét és teljesíthetőségét a 3.1.1 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 a Titkosító magánkulcs felhasználó személyes megjelenése, mert azonosítás-hitelesítését el kell végezni.

2.1.6 A Tanúsítványtárral (Címtárral) kapcsolatos feladatok és kötelezettségek

A jelen fejezetre a „Hitelesítés Szolgáltatási Szabályzat Fokozott Biztonságú Elektronikus Aláírás-hitelesítési Szolgáltatáshoz” c. dokumentum 2.1.6 fejezetének tartalma érvényes azzal a módosítással, hogy a titkosító tanúsítványokra vonatkozó Tanúsítványtárat a Szolgáltató 95,5 % rendelkezésre állási szinten teszi elérhetővé.

2.1.7 Az Igénylő, az Előfizető és Titkosító magánkulcs felhasználó feladatai és hatásköre

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

1. az Igénylő a Tanúsítvány igénylése előtt megismerni és elfogadni Szolgáltató általános szerződéses feltételeit és a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra, illetve a Titkosítás Hitelesítés Szolgáltatásra érvényes HSzSz-ét,
2. az Előfizető az Ügyfélkapcsolati Irodánál személyesen megjelenő Igénylőt, aki a Tanúsítványt és az ezzel kapcsolatos műveleteket igényli, meghatalmazással ellátni,
3. az Előfizető a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra, illetve a Titkosítás Hitelesítés Szolgáltatásra érvényes HSzSz-eket és az Általános Szerződéses Feltételeket az alkalmazásában álló vagy vele szerződéses kapcsolatban álló Titkosító magánkulcs felhasználókkal megismertetni, különösen a titkosító kulcsok biztonságos használatával, technikai feltételeivel és jogi következményeivel kapcsolatosan,
4. a Tanúsítvány igénylését és a kulcs-pár felhasználását úgy végezni, hogy a harmadik fél jogait ne sértse,
5. az Előfizető a Tanúsítvány kiadásához szükséges, a Titkosító magánkulcs felhasználókra vonatkozó adatokat ellenőrizni, ennek érdekében a Tanúsítvány kibocsátására vonatkozó kérelem érvényesítését megelőzően köteles a Titkosító magánkulcs felhasználót azonosítani,
6. az Előfizető teljes, pontos, valós és hiteles adatokat szolgáltatni a Szolgáltató részére az igényelni kívánt Titkosító tanúsítvány követelményeinek megfelelően a Titkosító magánkulcs felhasználó személyazonosságát, szervezeti identitását és a regisztrációhoz szükséges egyéb jellemzőket illetően,
7. az Előfizető és a Titkosító magánkulcs felhasználó megismerni a magánkulcsának átvétele és felhasználása előtt a magánkulcs tárolásával, az állományok titkosításával, illetve visszaállításával kapcsolatos technikai, jogi, biztonsági követelményeket és feltételeket,
8. a Titkosító magánkulcs felhasználó biztosítani a Kulcshordozó eszközének és adatának, valamint a Kulcshordozó eszköz és a transzport kulcs PIN kódjának védelmét,
9. a Titkosító magánkulcs felhasználó a magánkulcsát csak a titkosított állomány visszaállítására használni;

10. az Előfizető, illetve a Titkosító magánkulcs felhasználó 3 (három) munkanapon belül jelezni Szolgáltatnál a regisztráció során felvett adataiban történő változásokat, különös tekintettel a Tanúsítványba foglalt adatokra,
11. a jogi személy Előfizető a Titkosító magánkulcs felhasználói figyelmét külön felhívni arra, ha az Előfizetői Szerződés a Tanúsítvány felhasználhatóságával kapcsolatban összeg, területi vagy egyéb korlátozásokat köthet ki;
12. az Érintett fél, illetve az Előfizető a titkosító nyilvános, illetve magánkulcsokat csak a Tanúsítványban szereplő valamennyi korlátozásnak megfelelően használhatja,
13. a Titkosító magánkulcs felhasználó tudomásul venni, hogy magánkulcsának használata és védelme kizárólag a saját felelőssége, ezért ezzel - így különösen a magánkulcsának illetéktelen harmadik személyhez kerülésével - kapcsolatban a Szolgáltatót semmiféle felelősség nem terheli,
14. a jogi személy Előfizető megbízott kapcsolattartója tudomásul venni, hogy transzport magánkulcsának használata és védelme kizárólag a saját felelőssége, ezért ezzel - így különösen a magánkulcsának illetéktelen harmadik személyhez kerülésével - kapcsolatban a Szolgáltatót semmiféle felelősség nem terheli,
15. az Érintett fél tudomásul venni, hogy a Titkosító nyilvános kulcshoz tartozó Tanúsítvány ellenőrzésének elmulasztásából eredő következményekért az Érintett fél felel;

    érvénytelen vagy visszavont Tanúsítványhoz tartozó nyilvános kulccsal titkosító műveletet végrehajtani tilos,
16. a Titkosító magánkulcs felhasználó azonnal 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,
    - a Titkosító magánkulcs és/vagy a PIN kód nem a Titkosító magánkulcs felhasználó kizárólagos birtokában van (elveszett, ellopták, esetleg kompromittálták), vagy ennek alapos gyanúja áll fenn;
17. az Előfizető az Előfizetői Szerződésben rögzített szolgáltatási díjakat a Szolgáltatónak megfizetni,
18. a jogi személy Előfizető az ÁSzF módosításáról szóló értesítést követően a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz 2.1.7/15 pontjában meghatározott időn belül köteles a Titkosító magánkulcs felhasználóit írásban tájékoztatni a változások-

ról. Amennyiben az Előfizető nem fogadja el az ÁSzF módosítását, felmondási szándékát írásban kell bejelentenie a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz 2.1.7/14 pontjában meghatározott időn belül az illetékes regisztráló szervezetnél, amely a felmondás beérkezését követően, a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz 2.1.7/15 pontjában meghatározott időpontig kezdeményezi a Tanúsítvány visszavonását,

19. a Titkosító magánkulcs felhasználó vagy az Előfizető a titkosítási eljárással vagy a titkosított állománnyal kapcsolatos jogvita megindulásáról köteles haladéktalanul tájékoztatni a Szolgáltatót.

Ezeken kívül:

1. a Titkosító magánkulcs felhasználó jogosult arra, hogy a magánkulcsot birtokolja, és azt titkosított állományok visszaállítására (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 Érintett fél tudomásul veszi, hogy a Titkosító magánkulcs felhasználó Nyilvános kulcsával titkosított állományt saját felelősségére készíti, és viseli ennek esetleges jogkövetkezményeit;
4. az Érintett fél a Tanúsítványt csak a HP-nek, a Titkosítás Hitelesítés Szolgáltatásra érvényes HSzSz-nek megfelelően használhatja; titkosított állomány csak Tanúsítvány érvényességi ideje alatt készíthető.

2.1.8 Érintett fél feladatai és hatásköre

A titkosítás előtt az Érintett fél kötelessége a Szolgáltató szabályzatainak megfelelően a legnagyobb gondossággal eljárni a Titkosító magánkulcs felhasználó Nyilvános kulcsához tartozó Tanúsítvány elbírálásakor, ezen belül:

1. A Tanúsítvány elfogadása előtt meg kell értenie a titkosítással kapcsolatos technikai, jogi, biztonsági és egyéb vonatkozásokat.
2. Meg kell ismernie Szolgáltató nyilvánosan elérhető szabályzatait (a jelen HSzSz-t a Titkosítás Hitelesítés Szolgáltatásra, illetve a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz-t és ÁSzF-et). A titkosítási eljárásnak a titkosítandó állományon történő alkalmazása a Szolgáltató ezen szabályzatainak elfogadását jelenti.

3. A Tanúsítványban feltüntetett azonosító alapján, és egyéb törvényesen rendelkezésre álló adatok és módszerek segítségével a Titkosító magánkulcs felhasználó személyéről egyértelműen meg kell győződnie.
4. A Tanúsítvány érvényességét és hatályosságát ellenőriznie kell a nyilvánosan elérhető Tanúsítványban.
5. 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 a Titkosító magánkulcs felhasználó Tanúsítványának integritásáról meg kell győződnie.
   - A Tanúsítvány állapotát ellenőriznie kell a Tanúsítvány visszavonási listák (CRL) áttanulmányozásával.
   - Át kell tanulmányoznia a Tanúsítvány összes attribútumát, közöttük a korlátozó feltételeket is, és az adott titkosítási akcióra vonatkozó előírásoknak, valamint józan megfontolásoknak megfelelően döntést hozni a titkosítás megkezdéséről.
6. A titkosítási akciót az Érintett fél nem indíthatja el, ha a Titkosító magánkulcs felhasználó Nyilvános kulcsának Tanúsítványa, vagy a tanúsítási lánc tanúsítványainak valamely adata annak érvénytelenségére utal, illetve ha az az adott kontextusban nem fogadható el.

2.2 A hitelesítés szolgáltató és felhasználó közösség tagjainak felelőssége

2.2.1 A MÁV INFORMATIKA Kft. felelőssége

Általános Szabály

A MÁV INFORMATIKA Kft., mint Szolgáltató azzal, hogy aláír egy, a jelen HSzSz 1.4 pontja szerint meghatározott titkosító Tanúsítványt – és ezzel jelzi az 1.3.5 pontban meghatározott felhasználói közösség és az érintett felek felé ezen HSzSz használatát –, csak azért vállalja a felelősséget, hogy a Tanúsítvány előállítása, kibocsátása, közzététele, visszavonása és a Visszavonási Lista közzététele a jelen HSzSz-ben előírtaknak teljes mértékben megfelel, és a Szolgáltató megteszi a szükséges intézkedéseket ahhoz, hogy maga és az előfizetők is a jelen HSzSz előírásainak megfelelően járjanak el.

A Szolgáltató a szolgáltatásaival kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben kizárólag a saját hibájából, kötelezettségeinek megszegéséből,

valamint a neki felróható okokból bekövetkező, bizonyítható károkért tartozik helyt állni. Általában a Szolgáltató nem vállal felelősséget, ha a Szolgáltató által kibocsátott Tanúsítvány a jelen HSzSz-ben előírtaktól eltérő módon kerül felhasználásra. Így a Szolgáltató nem felelős az olyan károkért, mely abból adódott, hogy az Érintett fél a tanúsítványok ellenőrzése és felhasználása során nem a jelen HSzSz szerint járt el, illetve nem tanúsította a tőle elvárható gondosságot.

A Szolgáltató felelősségére a következő részletes szabályok mérvadók:

- Amennyiben a jelen HSzSz szabályai megszegésével a Szolgáltató a vele szerződéses jogviszonyban nem álló Érintett félnek kárt okoz, vagy a Tanúsítvány Érintett fél általi, – a HSzSz szerint történő – felhasználása ellenére, az Érintett fél kárt szenved, azért a Magyar Köztársaság Polgári Törvénykönyvéről szóló 1959. évi IV. törvény 339. §-ának megfelelően a Szolgáltató felelős, azzal a korlátozással, hogy a kártérítés mértéke Tanúsítvány típusonként és egyedi tanúsítványonként is maximált összegű az Általános Szolgáltatási Feltételek vagy az Előfizetői Szerződés vonatkozó feltételei szerint.
- A Szolgáltató köteles a Tanúsítvány megfelelő mezőjében feltüntetni, ha az Előfizetői Szerződésben a Tanúsítvány felhasználhatóságával kapcsolatban összegszerű, területi vagy egyéb korlátozásokat köt ki. Ezen korlátokat meghaladó ügyletekben felvetett követelésekért, illetve az így okozott kárért a Szolgáltató nem felel.
- A Szolgáltató kizárja felelősségét, ha az aláírás ellenőrzés lépései a HSzSz-ben meghatározott módon bármi okból – beleértve Szolgáltatónál keletkező működtetési és/vagy menedzselési problémát is – nem hajthatók végre a titkosítási művelet elindításának időpontjában, és a műveletet az Érintett fél ennek ellenére megvalósítja.
- Szolgáltató a HSzSz 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 szervezetek működéséért.

A 2. szintű (produktív) Hitelesítő Központ felelőssége:

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

2.2.3 Hitelesítési Politika és Szabályozási Csoport felelőssége

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 2.2.3 fejezetének tartalma érvényes.

2.2.4 A Regisztrációs Iroda felelőssége

A Regisztrációs Iroda felelős:

- a regisztrációs adatok ellenőrzéséért,
- az általa generált titkosító kulcspárok megfelelőségéért, a Titkosító magánkulcs, a Nyilvános kulcs és a Tanúsítvány összetartozásáért és a Tanúsítvánnyal együtt történő Kulcshordozó eszközre írásért,
- az Kulcshordozó eszköz és az aktivizáló (PIN) kód összetartozásáért.

2.2.5 Az Ügyfélkapcsolati Iroda felelőssége

- A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változatának 2.2.5 fejezetének tartalma érvényes.

2.2.6 Előfizető és a Titkosító magánkulcs felhasználó felelőssége

Az Előfizetőnek és a Titkosító magánkulcs felhasználónak büntetőjogi felelőssége áll fenn 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 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 tartásával számára okoz. A Titkosító magánkulcs felhasználó felelős azért, ha magánkulcsát nem a HSzSz-ben, az ÁSzF-ben és a vonatkozó jogszabályokban meghatározott módon és célra használta.

Az Előfizető és a Titkosító magánkulcs felhasználó felelős a magánkulcs biztonságos megőrzéséért, a kulcs tartalom és a PIN kód illetéktelenek tudomására jutásának megakadályozásáért.

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.

2.2.7 Érintett fél felelőssége

Érintett fél felelőssége fennáll a titkosító Tanúsítvány elfogadásából fakadó bármely következményért és kárért, ha a titkosító Tanúsítvány érvényességének és hatályosságának ellenőrzése során nem a jelen HSzSz szerint jár el.

Az Érintett fél felelős a Szolgáltató által kibocsátott titkosító tanúsítványok elfogadása során tanúsított körültekintő ellenőrzésért, valamint a Szolgáltató nyilvánosan elérhető szabályzatai rá vonatkozó részeinek megismeréséért, a szabályzatokban meghatározott kötelezettségeinek betartásáért.

2.3 A pénzügyi felelősség korlátjai

2.3.1 Kártérítés

A Szolgáltató nem felelős az olyan kárért, amely abból adódott, hogy az Érintett fél a tanúsítványok hitelességének és érvényességének ellenőrzésénél nem a jelen HSzSz és az általános szerződési feltételek szerint járt el, illetve nem tanúsította a tőle elvárható gondosságot.

A Titkosító magánkulcs, illetve Kulcshordozó eszköz illetéktelen kezekbe kerülés esetén a Szolgáltató nem felelős egészen az Előfizető vagy Titkosító magánkulcs felhasználó által tett bejelentés

időpontjáig azért a kárért, amely abból származik, hogy az Előfizető, illetve a Titkosító magánkulcs felhasználó nem a HSzSz-ben előírt biztonságos feltételek mellett tárolta, használta a Titkosító magánkulcsot, illetve Kulcshordozó 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 korlátait – kártérítés felső határa - az ÁSzF, illetve az Előfizetői Szerződés szerint kell értelmezni. Szolgáltató – helytállási kötelezettsége esetén – csak az ÁSzF-ben, illetve az Előfizetői Szerződésben megjelölt összeghatárig köteles kártérítésre.

A Szolgáltatással kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben a Szolgáltató a saját hibájából és a kötelezettségei megszegéséből, neki felróható okból bekövetkező bizonyítható károkért tartozik helyt állni.

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

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 2.3.2 fejezetének tartalma érvényes.

2.3.3 Adminisztratív eljárások

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

A Szolgáltató Szervezeti és Működési Szabályzatában kerültek meghatározásra azok az adminisztrációs folyamatok, amelyek a Kulcshordozó eszköz és a titkosító Tanúsítvány kibocsátást támogatják.

Ilyenek:

- Az igénylők adatainak nyilvántartása, tárolása, archiválása,
- Az Előfizetők, Titkosító magánkulcs felhasználók tanúsítványainak, a Visszavonási listák tárolása, archiválása,

- Számlázás, számlázási adatok nyilvántartása, archiválása,
- A Szolgáltató által üzemeltetett PKI rendszer elemeinek nyilvántartása,
- Hitelesítési tevékenység és biztonsági audit eljárások,
- Minőségbiztosítási eljárások.

2.4 Értelmezés és alkalmazás

2.4.1 Alkalmazott jogszabályok

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

- a hitelesítés szolgáltatás vonatkozásában 2001. évi XXXV. törvény az elektronikus aláírásról,
- az üzleti titkok vonatkozásában az 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról,
- a személyes adatok vonatkozásban az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról és az 1995. évi CXXII. törvény a polgárok személyes adatainak nyilvántartásáról szóló 1992. évi LXVI. tv. Módosításáról

szerint jár el.

Szolgáltató figyelembe veszi még 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

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 2.4.2.1 fejezetének tartalma érvényes.

2.4.2.2 Hatályosság

Jelen HSzSz időbeli hatálya az 1.3.6.1 pontnak megfelelően a hatálybaléptetéstől a szolgáltatási tevékenység megszűnéséig tart. Személyi és tárgyi hatályát a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változatának 1.3.6.1 pontja tartalmazza.

Jelen HSzSz 1.3.6.1. fejezete érvényben marad a HSzSz hatályának végét követően is (a hatályosság megszűnésének módjától függetlenül) mindazon tanúsítványokkal kapcsolatosan, amelyeket a Szolgáltató titkosító tanúsítványként bocsátott ki.

2.4.2.3 Megszűnés

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 2.4.2.3 fejezetének tartalma érvényes.

2.4.2.4 Értesítések

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 2.4.2.4 fejezetének tartalma érvényes.

2.4.3 Vitás kérdések kezelése

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 2.4.3 fejezetének tartalma érvényes.

2.5 Díjak

A mindenkor érvényes szolgáltatási díjakat a Szolgáltató az Ügyfélkapcsolati Irodában teszi hozzáférhetővé.

Az előfizetőkre vonatkozó hatályos szolgáltatási díjak az Előfizetői Szerződésben kerülnek rögzítésre

.A Szolgáltató jogosult az árlistát egyoldalúan módosítani.

Azok az előfizetők, akik a módosítást nem fogadják el, jogosultak az Előfizetői Szerződésüket legkésőbb a módosítás életbe lépésének napjáig 30 napos felmondási idővel felmondani. A szerződés felmondása egyben a kiadott Tanúsítvány iránti visszavonási kérelemnek is tekintendő és a Szolgáltató jogosult a Tanúsítványt Tanúsítványtárából törölni.

A fizetési feltételeket az ÁszF tartalmazza.

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

2.5.1 Tanúsítvány kibocsátás és megújítás

Szolgáltató a kibocsátott tanúsítványokért évente fizetendő éves fenntartási díjat számol fel az Előfizető felé, amely tartalmazza a Tanúsítvány kibocsátásának, Tanúsítványtárban történő közzétételének a díját az érvényesség időtartamára (5év). A Szolgáltató díjfizetés ellenében vállalja a Tanúsítvány érvényességi idejének lejárta, illetve esetleges visszavonása után a Tanúsítvány és a Titkosító kulcspár biztonságos megőrzését és tárolását és szükség esetén, - a korábbi állományok visszaállítása érdekében - a Tanúsítvány és a Titkosító magánkulcs kiadását az Előfizetőnek. A Tanúsítvány újbóli kiadása minden esetben díjfizetés ellenében történik. Ez alól csak a Tanúsítvány legelső kiadása kivétel, amely ingyenes.

2.5.2 Tanúsítvány hozzáférés

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

2.5.3 Visszavonás és állapot információ hozzáférés

Szolgáltató a közzétett visszavonási információ eléréséért nem számol fel díjat az érintett felek irányába.

2.5.4 Egyéb szolgáltatásokra vonatkozó díjak

Szolgáltató a kibocsátott tanúsítványok visszavonásáért, felfüggesztéséért és újraérvényesítéséért eljárási díjat számol fel az Előfizető felé, mely tartalmazza a Tanúsítvány megváltozott állapotának a Tanúsítványtárban történő közzétételének díját.

2.5.5 Visszatérítési elvek

Az Előfizető a számára kibocsátott Tanúsítvány éves fenntartási díjának visszakérésére 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 Kulcshordozó eszközön szereplő adatok a Szolgáltató hibájából fakadóan nem megfelelők,[8]
- a kibocsátott Kulcshordozó eszköz, az aktivizáló kód és a kulcsok nem összetartozók,
- a Szolgáltató egyéb hibát követ el a Tanúsítvány kibocsátásakor,

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

- a Szolgáltató bizonyítottan nem tartja be valamely kötelezettségét az Előfizető Tanúsítványának kezelésekor.

A díj visszatérítésére az Előfizetőnek a Tanúsítvány kibocsátását, illetve megújítását követő 30 naptári napon belül a regisztrációt végző regisztráló szervezetnél kérvényt[9] kell beadnia a Szolgáltató részére. A kérvény pozitív elbírálása esetén a Szolgáltató a Tanúsítványt díjmentesen visszavonja és a fenntartási díjat az Előfizető számára a megjelölt bankszámlaszámra 20 banki 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.

Szolgáltató egyéb tevékenységeiért számlázott díjak esetében díjvisszafizetésre nem köteles.

2.6 Közzététel

2.6.1 Szolgáltatói információk közzététele

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 2.6.1 fejezetének tartalma érvényes.

A Szolgáltató által kibocsátott tanúsítványok közzétételi módszereire vonatkozó rész a következőre módosul:

- A Titkosító magánkulcs felhasználó részére elküldi védett kommunikációs protokollt alkalmazva.
- A Titkosító magánkulcs felhasználó részére átadja a Kulcshordozó eszközön.
- Az érintett felek részére közzéteszi a nyilvános Tanúsítványtárában, amennyiben ehhez a Titkosító magánkulcs felhasználó és az Előfizető hozzájárult (a hozzájárulás formája a tanúsítványigénylő űrlapon ennek írásos jelölése).

2.6.2 A közzététel gyakorisága

- A Szolgáltató a kibocsátott titkosító tanúsítványokat a Tanúsítványtárban publikálja a 2.6.4 pontban megadott elérhetőséggel. A felfüggesztett és visszavont tanúsítványok visszavonási listáját a 4.4.9 pontnak megfelelő gyakorisággal tesz közzé.

[9] Erre vonatkozóan a Szolgáltatónak formanyomtatvánnyal rendelkezik.

- A Szolgáltató az egyes titkosító tanúsítványok nyilvánosságra hozatala kapcsán a következő gyakorlatot követi:
  - A Szolgáltató a végfelhasználói tanúsítványokat a kibocsátást követően, a regisztrációs eljárás részeként átadja az Előfizető részére.
  - A Szolgáltató a végfelhasználói tanúsítványokat a kibocsátást követően a Tanúsítványtárában 24 órán belül teszi közzé.
  - A Szolgáltató az általa működtetett hitelesítő egységek (CA-k) szolgáltatói Tanúsítványait Tanúsítványtárában a kibocsátást követő 24 órán belül teszi közzé.
  - A Szolgáltató az általa működtetett hitelesítő egységek (CA-k) szolgáltatói Tanúsítványait Internetes honlapján 5 munkanapon belül megjeleníti.
  - A Hitelesítő Központok Tanúsítványainak alkalmazásokban való megjelenése esetleges.

2.6.3 Elérési szabályok

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 2.6.3 fejezetének tartalma érvényes.

2.6.4 Tanúsítványtár (Címtár)

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

A Tanúsítványtár a *http://www.mavinformatika.hu/ca* web lapon érhető el.

2.7 A megfelelőség vizsgálata

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

1. a saját szervezetén belüli, a Szolgáltató egységtől független, belső auditor szervezettel,
2. független külső auditor céggel.

A Szolgáltató szolgáltatási rendszerének következő elemeit vizsgáltatja:

- Kulcshordozó eszközöket, melyeket magánkulcsainak tárolására használ.
- Kulcshordozó eszközöket, melyeket az előfizetők számára biztosít.
- A végfelhasználói és szolgáltatói tanúsítványok kezeléshez felhasznált elektronikus aláírási termékeit.
- A végfelhasználói és szolgáltatói tanúsítványok kezeléshez használt eljárásait és módszereit.

2.7.1 Vizsgálatok gyakorisága

A vizsgálatokat a Szolgáltató a Biztonsági Szabályzatában megjelölt rendszerességgel végzi, a törvényi feltételek vagy a szabályzataiban bekövetkezett jelentősebb változások esetén, saját döntése alapján, soron kívül végezteti el.

2.7.2 Az átvizsgáló szervezet megnevezése/jellemzői

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 2.7.2 fejezetének tartalma érvényes.

2.7.3 Az átvizsgáló szervezet és a vizsgált fél kapcsolata

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 2.7.3 fejezetének tartalma érvényes.

2.7.4 A vizsgálatok kiterjedése

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 2.7.4 fejezetének tartalma érvényes.

2.7.5 Hiányosságok kezelése

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 2.7.5 fejezetének tartalma érvényes.

2.7.6 Eredmény kommunikációja

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 2.7.6 fejezetének tartalma érvényes.

2.8 Bizalmasság – Adatkezelési szabályzat

2.8.1 Bizalmas információk

A Szolgáltató gondoskodik a jogszabályoknak való megfelelésről. Ennek keretén belül:

- A titkosító magánkulcs tárolt példányát és 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),

- 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 hitelesítés-szolgáltató által történő nyilvántartásba vételéhez: regisztrálás, az alanyok 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 alany 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 a Titkosító magánkulcs felhasználóra vonatkozó információ bizalmas kezeléséről, kivéve, ha felfedésükhöz ők maguk[10] 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 a Titkosító magánkulcs felhasználók és a hitelesítés szolgáltatók magánkulcsai képezik, ezen belül a legérzékenyebb a szolgáltatói aláíró magánkulcs adat, mert kompromittálódása a Szolgáltató tevékenységének azonnali felfüggesztésével jár. Ezért ezeket az adatokat, illetve az ezeket hordozó eszközöket fokozott biztonsággal kell tárolni és használni. A Titkosító magánkulcs biztonságáért a teljes felelősséget az adat tulajdonosa viseli.

A Szolgáltató tevékenysége során a következő bizalmas adatköröket kezeli:

[10] vagy nevükben az Előfizető

1. a Szolgáltató üzleti titkai,
2. más Társaságok által a Szolgáltatónak átadott üzleti titkok,
3. az Előfizetők, a Titkosító magánkulcs felhasználók és a saját munkatársainak személyes adatai.

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 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 a Titkosító magánkulcs felhasználók személyes adatait csak a közöttük fennálló Előfizetői Szerződéssel összhangban levő célokra használhatja fel, harmadik félnek azokat az Előfizetők és a Titkosító magánkulcs felhasználók 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 a Titkosító magánkulcs felhasználó a Tanúsítvány igénylésével hozzájárul ahhoz, hogy a Szolgáltató személyes adatait (a Titokvédelmi és a Biztonsági Szabályzatainak megfelelő módon) tárolja és kezelje. A hozzájárulás egyaránt vonatkozik az adatok alannyal és Előfizetővel való megosztására (ha a két fél különbözik), s nyilvántartásba vett információk harmadik félhez történő továbbítására, a szolgáltató szolgáltatásainak leállítása esetén[11]. A tanúsítványigénylő űrlapon az Előfizetőnek és a Titkosító magánkulcs felhasználónak 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 Tanúsítványtárán keresztül nyilvánosságra kerül a nyilvános kulcs tulajdonosának azonosítása céljából,

[11] 2001. évi XXXV. Törvény az elektronikus aláírásról 16. § (2) bek.

másik részét a Szolgáltató védett módon tárolja az Előfizető és a Titkosító magánkulcs felhasználó azonosságának igazolása és egyéb adatszolgáltatási kötelezettségei céljából

2.8.2 Nem bizalmas információk

A Szolgáltató nem bizalmas információként kezeli mindazon adatokat, amelyeket a Tanúsítványba belefoglal[12]. Szerződéskötéskor az Előfizető és a Titkosító magánkulcs felhasználó tudomására kell hozni, hogy mely személyes adatai fognak a Tanúsítványtárban hozzáférhető tanúsítványokban szerepelni és a regisztrációs lapon ezeket külön jelölni kell.

Nem bizalmas adatok még azok a Szolgáltatóhoz kapcsolódó adatok is, amelyeket a Szolgáltató vezetője publikusnak minősít, illetve amelyekről a hatályos jogszabályok így rendelkeznek, pl. az ÁSzF és a HSzSz.

2.8.3 Tanúsítvány visszavonási és felfüggesztési okok felfedése

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 2.8.3 fejezetének tartalma érvényes.

2.8.4 Feltárás törvényi meghatalmazással rendelkezők részére

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

2.8.5 Információszolgáltatás polgári eljárás keretében

A Szolgáltató a Tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során - az érintettség igazolása esetén - a Titkosító magánkulcs felhasználó személyazonosságát igazoló adatokat átadhatja az ellenérdekű peres félnek vagy képviselőjének feltárhat bizalmas felhasználói információkat, illetőleg azt közölheti a megkereső bírósággal a 2001. évi XXXV. törvény 11.§ paragrafusa alapján. A Szolgáltató rögzíti az információszolgáltatás tényét, és arról tájékoztatja az Előfizetőt és a Titkosító magánkulcs felhasználót.

[12] Függetlenül attól, hogy az Előfizető hozzájárul-e (a Titkosító magánkulcs felhasználó nevében) a tanúsítvány nyilvánosságra hozásához.

2.8.6 Feltárás tulajdonos kérésére

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

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 a Titkosító magánkulcs felhasználó, 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 a Felhasználó részére kibocsátott egyedi azonosító a Szolgáltató tulajdonát képezi. A Tanúsítványban szereplő megkülönböztető név használatára a megnevezett Felhasználó jogosult.

A Titkosító magánkulcs felhasználó egyedi azonosítójában szereplő bármilyen védjegy, szervezeti- és személynév, vagy egyéb adat az Előfizető vagy a Titkosító magánkulcs felhasználó 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 a kezdeti regisztrálás során:

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

3.1.1 Nevek típusa

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 3.1.1 fejezetének tartalma érvényes.

3.1.2 Név jelentése, szemantikája

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 3.1.2 fejezetének tartalma érvényes.

3.1.3 Különböző névmegadási formák értelmezési szabályai

A nevek formátumát az 1.4.1 fejezetben meghatározott tanúsítványfajták névmegadási szabályaival adtuk meg.

A névmegadási formák értelmezése érdekében érintett feleknek a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változatának 3.1.1 pontjában leírtak alapján kell eljárni. 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 a Titkosító magánkulcs felhasználó és az Előfizető egyéb adatairól többlettájékoztatást nem ad, csak a Tanúsítványban feltüntetett adatok értelmezését segíti.

3.1.4 Nevek egyedisége

A Szolgáltató biztosítja Tanúsítványtárában a tulajdonosazonosítók egyediségét. Erről elsődlegesen a Titkosító magánkulcs felhasználó e-mail címének a névmegadásban való szerepeltetése gondos-

kodik. 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 a Titkosító magánkulcs felhasználóra, de biztosítja a megkülönböztethetőséget.

A Szolgáltató biztosítja, hogy a teljes működési ciklusa alatt egy Tanúsítványban az általa használt megkülönböztetett nevet sohasem fogja egy másik egyedhez rendelni.

3.1.5 Név igénylési viták feloldása

A Titkosító magánkulcs felhasználót egyértelműen a Tanúsítványban megadott név és a Tanúsítvány sorozat száma különbözteti meg a többi Titkosító magánkulcs felhasználótól. Ezen kívül a névmegadásnál a Common Name mezőben a Titkosító magánkulcs felhasználó neve mellett az e-mail címe is szerepel, annak érdekében, hogy biztosított legyen a név megkülönböztetés, arra az esetre, ha Tanúsítvány sorozat száma és a Titkosító magánkulcs felhasználó 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 a Titkosító magánkulcs felhasználóra, de biztosítja a megkülönböztethetőséget.

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 a Titkosító magánkulcs felhasználó jogosultságát a feltüntetett nevek használatára. Szolgáltató fenntartja magának a jogot az igényelt nevek kiosztásának visszautasítására. Jogszerűtlen név- vagy adathasználat miatt, amennyiben erre bíróság kötelezi, vagy másik fél megalapozott módon bizonyítani tudja jogosultságát, a Szolgáltatónak jogában áll visszavonni a kérdéses Tanúsítványt.

3.1.6 Védjegyek elismerésének és hitelesítésének módszere

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 3.1.6 fejezetének tartalma érvényes.

3.1.7 A Titkosító magánkulcs birtoklás ellenőrzésének módszere

A Titkosító tanúsítványhoz tartozó titkosító kulcspár generálása a Szolgáltató Hitelesítő Központjában történik. Központi kulcs generálás esetén a Titkosító nyilvános és magánkulcs egymáshoz tartozásának, valamint a Titkosító magánkulcs birtoklásának ellenőrzésére nincs szükség, csupán a Titkosító magánkulcs felhasználóhoz eljutatott Kulcshordozó eszköz, illetve magánkulcs igazolására van szükség. A Kulcshordozó eszköz személyes átvételénél az Előfizető írásban igazolja a Kulcshordozó eszköz és a PIN kód átvételét. Az átvétel után az Előfizető és a Titkosító magánkulcs felhasználó teljes felelősséget visel a Kulcshordozó eszköz és a PIN kód biztonságos használatáért és megőrzésért.

3.1.8 Személyes azonosság hitelesítése „Személyes" tanúsítvány igénylése esetén

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 3.1.8 fejezetének tartalma érvényes.

3.1.9 Szervezeti identitás hitelesítése „Szervezeti személy" tanúsítvány igénylése esetén

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

A szervezeti személy hitelesítéséhez a következő adatokat kéri az Ügyfélkapcsolati Iroda:

- az igénylő szervezet neve, székhelye,
- annak a szervezeti egységnek a megnevezése, ahol a szervezeti személy (továbbiakban: Titkosító magánkulcs felhasználó) dolgozik,
- a Titkosító magánkulcs felhasználó neve, aláírása,
- a Titkosító magánkulcs felhasználó beosztása (az előfizető szervezet és szervezeti egység viszonya a Titkosító magánkulcs felhasználóhoz)
- a Titkosító magánkulcs felhasználó személyi igazolvány vagy útlevél száma,
- a Titkosító magánkulcs felhasználó telefon száma, e-mail címe.
- a Titkosító magánkulcs felhasználót megbízó dokumentum cégszerűen aláírva (a dokumentum tartalmazza a megbízó szervezet vagy szervezeti egység nevét, e-mail címét, telefon és fax számát),

- az előfizető szervezet egyértelmű hozzájárulása ahhoz, hogy:
  - a Tanúsítvány kibocsátásra kerüljön,
  - a szervezet vagy szervezeti egysége neve a Tanúsítvány tulajdonosazonosító mezőjében feltüntetésre kerüljön,
  - a Titkosító magánkulcs felhasználó 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 a Titkosító magánkulcs felhasználó részére történő Tanúsítvány kibocsátásához,
  - az Előfizető kapcsolattartókat nevez meg a Szolgáltató részére, akik hagyományos és elektronikus aláírási joggal rendelkeznek a Tanúsítvány kibocsátását illetően; a Szolgáltató később e személyeknek az aláírását fogadja el bármilyen kérelem vagy bejelentés esetén,
  - az előfizető szervezet 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 Titkosító magánkulcs felhasználó kijelölését engedélyező személy neve (az engedélyezőnek minden esetben cégképviseletre jogosult személynek kell lennie és ezt aláírási címpéldánnyal kell igazolni),
- az engedélyező személy beosztása,
- az engedélyező személy munkahelyi telefonszáma, fax-száma, e-mail címe.

Ezen adatokat a következő dokumentumokkal kell hitelesíteni:

- képviseleti megbízás cégszerűen aláírva,
- A Kapcsolattartó azonosítás-hitelesítése személyi igazolvány vagy útlevél bemutatásával személyesen
- A Titkosító magánkulcs felhasználó(k) azonosítás-hitelesítése személyi igazolvány vagy útlevél bemutatásával személyesen; A Szolgáltató eltekint a Titkosító magánkulcs felhasználó(k) sze-

mélyes azonosítás-hitelesítésétől abban az esetben, ha ezt az előfizető szervezet elvégezte és a képviseleti megbízásban írásban igazolja. A Titkosító magánkulcs felhasználó(k) azonosítás-hitelesítéséhez kapcsolódó minden felelősség ebben az esetben az előfizető szervezetre hárul.

- 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 címpéldány, 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. Szervezeti személy típusú tanúsítvány igénylés esetén az Ügyfélkapcsolati Iroda az aláírási jogosultság ellenőrzése céljából adategyeztetést végezhet a cégnyilvántartással[13].

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

- az okmányok személyhez tartozásával, eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel,
- a bemutatott dokumentumok 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.

[13] 2001. évi XXXV. törvény 12. § (2) b)

3.1.10 Eszköz identitás hitelesítése

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 3.1.10 fejezetének tartalma érvényes.

3.2 Érvényes Tanúsítvány megújítása (Tanúsítvány frissítése)

Egy érvényes (nem lejárt és nem visszavont) Tanúsítvány megújítására a szolgáltató az alábbi lehetőséget biztosítja:

- Tanúsítvány kulcscsere, melynek során a Szolgáltató az érvényes aláíró magánkulcsával írja alá az új titkosító Tanúsítványban a Tanúsítvány alanyának új nyilvános kulcsát és változatlan egyéb adatait új érvényességi időtartamra.

  Tanúsítványának lejárta előtt, az Előfizető az Előfizetői Szerződésben meghatározott időpontban (ha a Szerződés erről nem intézkedik, akkor a lejárat előtt 15 nappal korábban) e-mailben kap értesítést a Szolgáltatótól a Tanúsítvány megújítás szükségességéről.

  A Szolgáltató által kibocsátott előfizetői tanúsítványok érvényességi ideje 5 év, amelyet a lejárat után még 5 évig (vagyis összesen 10 évig) lehet meghosszabbítani.

Előfizetői tanúsítvány megújítása csak akkor lehetséges, ha:

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

Ha mindezen feltételek nem teljesülnek, a tanúsítvány alanyának új Tanúsítványt kell igényelnie a kezdeti regisztráció módszerével.

3.3 Érvénytelen Tanúsítvány megújítása

Ha a Tanúsítvány vissza lett vonva vagy az érvényessége lejárt, akkor a Tanúsítvány megújítása új Tanúsítvány igényelésével történik, a regisztrációs eljárás újbóli végrehajtásával.

3.4 Felfüggesztés és visszavonási kérés

Felfüggesztés és visszavonási kérés személyes megjelenéssel vagy hitelesített elektronikus üzenetváltással történhet. A Tanúsítvány visszavonási kérés azonosítási és hitelesítési vonatkozásai megtalálhatók a 4.4 fejezetben.

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

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

4. A működésre vonatkozó követelmények

4.1 Tanúsítványigénylés

Tanúsítvány a Szolgáltatótól az Ügyfélkapcsolati Irodánál igényelhető, az adott tanúsítvány osztálynak megfelelő, a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz 3.1.8 és 3.19 pontjaiban 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 használatával kapcsolatos kikötésekről és feltételekről a jelen HSzSz 3.1.8 és 3.19 pontjaiban megadottak szerint. A kapcsolatfelvételkor – amennyiben az Igénylő Titkosító magánkulcs és kulcshordozó 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[14] és kitölthető. Amennyiben az Előfizető igényli, az Ügyfélkapcsolati Iroda az egyéb nyilvános dokumentumok tanulmányozásának lehetőségét is biztosítja, valamint szóban válaszol az Igénylőnek 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.

c. A Szolgáltató a Titkosító magánkulcs felhasználót 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.

[14] 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.

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 jelen HSzSz 3.1.8 és 3.19 pontjaiban 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. A Titkosító magánkulcs felhasználó azonosítójának (egyedi nevének) megállapítása a 3.1 pontban tárgyaltaknak megfelelően történik.

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 a Kulcshordozó eszköz használatát, védelmét,
   - garantálja feltüntetett adatainak valódiságát,
   - az adatok későbbi változásairól a Szolgáltatót értesíti.

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

k. A Tanúsítványigénylő űrlapot az Ügyfélkapcsolati Iroda nyilvántartásába veszi és archiválja.

l. Az Ügyfélkapcsolati Iroda nyilvántartásba veszi az Előfizetővel aláírt nyilatkozatokat[15], beleértve az alábbiakat:

- az Előfizető kötelezettségeivel (lásd 3.1.9) történő egyetértést,
- az Előfizető beleegyezését a Kulcshordozó eszköz használatára vonatkozóan,
- hozzájárulás az alábbi szolgáltatások során felhasznált adatok Szolgáltató által történő nyilvántartásba vételéhez: regisztrálás, az előfizetők eszközzel való ellátása (beleértve az Előfizetőhöz történő továbbítást is), bármely ezt követő visszavonás, illetve ezen információk harmadik félhez történő továbbítása (a Szolgáltató szolgáltatásainak leállítása esetén HSzSz által megkövetelt feltételek szerint),
- hogy az Előfizető megköveteli-e, a Titkosító magánkulcs felhasználó pedig hozzájárul-e a Tanúsítvány közzétételéhez és milyen feltételek mellett,
- annak megerősítését, hogy a Tanúsítványban szereplő adatok helyesek[16].

A Szolgáltató megőrzi a d)-f) pontokban megnevezett nyilvántartásokat 10 évig[17], 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.

4.2 Tanúsítvány kibocsátás

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

- az Előfizető, a Titkosító magánkulcs felhasználó vagy az eredetileg regisztrált képviselője személyesen átveheti az Ügyfélkapcsolati Irodán, vagy
- utólagosan letöltheti a nyilvános Tanúsítványtárból

[15] 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 megköthető.
[16] A fenti megállapodás elektronikus formát is ölthet.
[17] A 2001. évi XXXV. törvény 9. § (7) pontja legalább 10 év megőrzési időt követel meg.

A Szolgáltató biztonságosan fenntartja az általa kibocsátott tanúsítványok hitelességét a következő módon:

- Előállítása után a teljes és pontos Tanúsítvány rendelkezésére áll azon Előfizető vagy Titkosító magánkulcs felhasználó számára, akinek a Tanúsítvány kibocsátásra került.
- A Tanúsítvány kibocsátás eljárása biztonságosan kapcsolódik a megfelelő regisztrációhoz, illetve a különböző tanúsítvány megújítási eljárásokhoz.
- A Titkosító magánkulcs felhasználó számára a Szolgáltató által megvalósított kulcspár előállításra:
  - a Tanúsítvány kibocsátás eljárása biztonságosan kapcsolódik a Szolgáltató általi kulcspár előállításhoz;
  - a Titkosító magánkulcs felhasználó Titkosító magánkulcsát tartalmazó Aláírás létrehozó eszközt biztonságosan továbbítják az Előfizetőhöz.

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

- az Igénylő benyújtotta kérelmét a Regisztrációs Irodának,
- a Titkosító magánkulcs felhasználó (akinek nevében az Igénylő eljár, amennyiben nem azonos a Titkosító magánkulcs felhasználóval) azonos a kérelemben szereplő alannyal (subject),
- az Igénylő jogosult a kérelemben szereplő Titkosító magánkulcs felhasználó nevében kérelmet benyújtani,
- a Regisztrációs 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 felvett elektronikus űrlap alapján végzi a Hitelesítő Központ.

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

4.3 Tanúsítvány elfogadás

A Regisztrációs Iroda, a Szolgáltató felelősségi körében eljárva az elkészült Tanúsítványt ellenőrzi, Kulcshordozó eszközre írja a Titkosító magánkulccsal együtt, majd az eszközt és a PIN kódot személyesen adja át az Ügyfélkapcsolati Irodában megjelent Előfizetőnek.

Előfizetői szerződés megkötése esetén az átadás során átadásra kerül:

- a Kulcshordozó eszköz, rajta a Titkosító magánkulccsal és a Tanúsítvánnyal,
- az aláírt regisztrációs űrlap egy eredeti példánya,
- a tájékoztató brosúra,
- az aláírt Előfizetői Szerződés egy példánya.

A Kulcshordozó eszköz átvételének megtagadása visszavonási kérelemnek számít.

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

A személyes, illetve postai úton történő átadásnál a Kulcshordozót kizárólag a regisztrációs űrlapon megjelölt Titkosító magánkulcs felhasználó, illetve Eszköz tanúsítvány esetén az Előfizető írásban feljogosított meghatalmazottja veheti át.

A magánkulcs és a Tanúsítvány elfogadása a Titkosító magánkulcs első felhasználásával történik meg.

A Tanúsítvány elfogadásával együtt az Előfizetőnek írásban kell megerősíteni a következőket:

- ismeri, érti és elfogadja jelen és kapcsolódó nyilvánosan hozzáférhető szabályzatokat,
- 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 a Titkosító magánkulcshoz,
- ismeri a titkosító kulcsok megfelelő használatának módját, tisztában van azok technikai feltételeivel és jogi következményeivel,
- a Tanúsítványt kizárólag törvényes célokra, jogszerűen, a jelen és kapcsolódó szabályzatoknak és törvényi előírásoknak megfelelően használja,

- tisztában van azzal, hogy a Titkosító magánkulcs védelme kizárólag a Felhasználó felelőssége, s ezzel kapcsolatban a Szolgáltatót semmiféle felelősség nem terheli,
- felhatalmazza a Szolgáltatót a Tanúsítvány nyilvánosságra hozatalával, és saját vagy más nyilvános Tanúsítványtárakban történő elhelyezésével.

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

A Titkosító magánkulcs használatba vétele előtt az Előfizetőnek kötelessége ellenőrizni a Tanúsítványban feltűntetett adatainak helyességét. Amennyiben bármilyen rendellenességet talál a Titkosító magánkulcsot nem használhatja fel, hanem azonnal intézkednie kell a Tanúsítvány visszavonása érdekében.

4.4 Tanúsítvány visszavonás és felfüggesztés

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

A megsemmisítéséig a magánkulcs ugyanolyan felügyeletben részesítendő, mintha érvényes lenne.

A visszavonási/felfüggesztési kérelmek fogadását és azoknak a sikeres ellenőrzés utáni végrehajtását a Szolgáltató mindennap 24 órában, 95,5%-os rendelkezésre állással biztosítja úgy, hogy esetenként a visszavonási/felfüggesztési kezelés kiesése nem lehet több, mint 24 óra.

4.4.1 Visszavonáshoz vezető körülmények

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

- a magánkulcs kompromittálódása, vagy annak gyanúja,

- a Kulcshordozó eszköz elvesztése, eltulajdonítása, megrongálódása,
- a Kulcshordozó 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,
- a Titkosító magánkulcs felhasználónak a Tanúsítványban feltűntetett adatainak megváltozása,
- a Tanúsítványban feltűntetett szervezet adatainak megváltozása,
- a Tanúsítványban feltűntetett Titkosító magánkulcs felhasználó és szervezet kapcsolatának megváltozása vagy megszűnése

miatt.

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

A Szolgáltató kezdeményezése alapján a Tanúsítvány visszavonásra kerül, ha:

- a Tanúsítvány felfüggesztési ideje lejárt,
- az Előfizető és/vagy a Titkosító magánkulcs felhasználó az ÁszF-et, Előfizetői Szerződést megszegi,
- az Előfizető és/vagy a Titkosító magánkulcs felhasználó kötelezettségeiket nem tartják be,
- az Előfizetői szerződés megszűnik,
- a Szolgáltató tudomására jutott tény, vagy alapos gyanú, a regisztrációs adatok valótlanságáról,
- a Tanúsítványban feltűntetett kibocsátó adatok megváltoznak,
- a hitelesítési szolgáltatás megszűnik,
- a Regisztrációs Iroda megszűnik,
- a Szolgáltató valamely magánkulcsának kompromittálódik.

Egyéb visszavonáshoz vezető körülmények:

- harmadik fél, pl. Érintett fél kezdeményezi.
- a Titkosító magánkulcs felhasználó halála, az Előfizető megszűnése,

4.4.2 Visszavonás kérelmezése

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 4.4.2 fejezetének tartalma érvényes.

4.4.3 Visszavonási eljárás

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

- természetes személy Előfizető esetén maga a Titkosító magánkulcs felhasználó vagy az általa megbízott és a Szolgáltató által nyilvántartott képviselője,
- jogi személy Előfizető esetén maga a Titkosító magánkulcs felhasználó vagy a jogi személy által megbízott és a Szolgáltató által nyilvántartott képviselő,

E-mail-el történő bejelentés esetén a Titkosító magánkulcs felhasználó Tanúsítványa érvényességének ellenőrzése után a bejelentés aláírás ellenőrzése hitelesíti a Titkosító magánkulcs felhasználót.

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 felfüggesztési jelszóval 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-mail-ben 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.

4.4.4 Visszavonási kérelemre vonatkozó türelmi idő

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 4.4.4 fejezetének tartalma érvényes

4.4.5 Felfüggesztéshez vezető körülmények

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

- a magánkulcs kompromittálódásának gyanúja,
- a Kulcshordozó eszköz elvesztése, eltulajdonításának gyanúja,
- a Kulcshordozó eszköz eszközt védő aktivizáló adat (PIN kód) kompromittálódásának gyanúja miatt.

A felfüggesztési kérelmet mérlegelés nélkül teljesíteni kell, ha a Titkosító magánkulcs felhasználó, 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 szükség 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.

4.4.6 Felfüggesztés kérelmezése

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 4.4.6 fejezetének tartalma érvényes

4.4.7 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.

Amennyiben a kérelmet az Előfizető terjesztette be, a szolgáltatónak nincs mérlegelési joga a végrehajtás tekintetében. A bejelentett felfüggesztési kérelmeket a Regisztrációs Iroda a Hitelesítő Központnak továbbítja.

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

A felfüggesztési kérelem bejelentésének és végrehajtásának a Titkosító magánkulcs kompromittálódása esetén késlekedés nélkül, minden más műveletet megelőzve meg kell történnie az észlelést követően.

4.4.8 Felfüggesztett állapotra vonatkozó korlátozások

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 4.4.8 fejezetének tartalma érvényes.

4.4.9 CRL kibocsátás gyakorisága

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 4.4.9 fejezetének tartalma érvényes.

A fejezet utolsó mondata a következőre módosul:

„A visszavonási lista elérhetőségét a Szolgáltató minden nap 24 órában, 95,5%-os rendelkezésre állással biztosítja úgy, hogy az esetenkénti elérhetőség kiesése nem lehet több, mint 24 óra.”

4.4.10 CRL ellenőrzési követelmények

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 4.4.10 fejezetének tartalma érvényes.

4.4.11 On-line visszavonási státusz-szolgáltatás

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

4.4.12 On-line visszavonás ellenőrzési követelmények

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

4.4.13 Visszavonási állapot közlés más formái

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 4.4.13 fejezetének tartalma érvényes.

4.4.14 Visszavonási állapot közlés más formáinak ellenőrzési követelményei

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

4.4.15 Magánkulcs kompromittálódás speciális követelményei

A Titkosító magánkulcs kompromittálódása, vagy vélelmezett kompromittálódása esetén a Tanúsítvány visszavonásáról azonnal intézkedni kell. Alapos gyanú esetén a Titkosító magánkulcs használatát azonnal fel kell függeszteni.

A kompromittálódott Titkosító magánkulcs a megsemmisítéséig ugyanolyan felügyeletben részesítendő, mint egy érvényes Titkosító magánkulcs.

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

4.5 Biztonsági audit eljárások

A Szolgáltató hitelesítés-szolgáltatást támogató informatikai rendszerének biztonsági naplózását és annak auditálását a jelen HSzSz mellett a Szolgáltató biztonsági szabályzata szabályozza részletesen.

4.5.1 Naplózott esemény típusok

A Szolgáltató hitelesítés támogató informatikai rendszerén az 5.3 pontban meghatározott szerepkörű munkatársai által végzett műveletek naplózásra kerülnek, amelyeket a regisztráció, a tanúsítványigénylés, a titkosító kulcspár generálása, a Kulcshordozó eszköz megszemélyesítése, a Tanúsítvány létrehozása és kibocsátása 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 tanúsítványok életciklusával kapcsolatos összes eseményt.

A Titkosító magánkulcs felhasználók kulcshordozó eszközzel való ellátásával kapcsolatosan[18]:

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

A visszavonás kezeléssel kapcsolatosan a Szolgáltató gondoskodik a visszavonással kapcsolatos összes kérés, valamint az ezek eredményét képező összes tevékenység naplózásáról. A naplóbejegyzések a bejegyzés pontos idejét, a tevékenység időpontját (ha az a bejegyzés idejétől eltér) és végrehajtóját is tartalmazzák.

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

4.5.2 Napló adatok feldolgozásának gyakorisága

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 4.5.2 fejezetének tartalma érvényes.

4.5.3 Napló adatok tárolási ideje

A naplózások havonta egyszer kerülnek archiválásra a szükségessé váló visszakeresés céljából. Az archivált naplókat keletkezésüktől számított 10 évig kerülnek megőrzésre.

4.5.4 Napló adatok védelme

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 4.5.4 fejezetének tartalma érvényes.

4.5.5 Napló adatok mentési eljárásai

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 4.5.5 fejezetének tartalma érvényes.

[18] Az „Titkosító magánkulcs elhelyezése kulcshordozó eszközön” szolgáltatás keretén belül.

4.5.6 Napló adatok gyűjtési rendszere

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 4.5.6 fejezetének tartalma érvényes.

4.5.7 Rendkívüli eseményekről történő értesítés

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 4.5.7 fejezetének tartalma érvényes.

4.5.8 Sebezhetőség kiértékelése

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 4.5.8 fejezetének tartalma érvényes.

4.6 Adatarchiválás

A Szolgáltató gondoskodik arról, hogy a Tanúsítványra vonatkozó minden lényeges adat és információ megfelelő ideig rögzítésre kerüljön, különösen jogi eljárásokhoz bizonyíték nyújtása érdekében[19].

4.6.1 A tárolt események típusai

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 4.6.1 fejezetének tartalma érvényes.

4.6.2 Az archívum megőrzési időtartama

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 4.6.2 fejezetének tartalma érvényes.

4.6.3 Az archívum védelme

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 4.6.3 fejezetének tartalma érvényes.

[19] A tanúsítványokra vonatkozó archivált rekordok regisztrációs adatokat és a Szolgáltató környezeti, kulcs- és tanúsítvány gondozási eseményeire vonatkozó fontos információkat tartalmaznak.

4.6.4 Az archívum mentési folyamatai

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 4.6.4 fejezetének tartalma érvényes.

4.6.5 A rekordok időbélyegzésére vonatkozó követelmények

Az archivált adatállományok időbélyegzővel vannak ellátva.

4.6.6 Az archívum gyűjtési rendszere

Az archivált adathordozók első példányai a Szolgáltató archívumában, a biztonsági példányai a Biztonsági Adattárban kerülnek elhelyezésre.

4.6.7 Archív információ hozzáférését és ellenőrzését végző eljárások

A Szolgáltató az archívumhoz Ügyfélkapcsolati Irodáján keresztül biztosít hozzáférést. A hozzáférés a Titkosító magánkulcs felhasználónak és az Előfizetőnek a rá vonatkozó adatokhoz lehetséges, más feleknek a 2.8.4 - 2.8.7 pontok szerint. A Szolgáltató a jogosultságot minden esetben ellenőrzi, és azt naplózza.

4.7 Kulcscsere

Kulcscsere és ezzel együtt új Tanúsítvány kibocsátása két esetben történik:

1. a Tanúsítvány érvényességi idejének lejártakor,
2. a Tanúsítvány visszavonása után.

Mindkét esetben az új Tanúsítvány kibocsátása akkor történik meg, ha azt az Előfizető igényli,

A Tanúsítvány érvényességi idejének lejártakor a Szolgáltató a lejáratot megelőzően intézkedik az új Titkosító magánkulcs előállításra. Az Előfizető igényének beérkezése után megkezdi részére az új magánkulccsal aláírt Tanúsítványok kiadását. A nem tervezett kulcs változtatás esetei a 4.8 pontban találhatók.

Szolgáltató által kibocsátott előfizetői titkosító tanúsítványok érvényességi ideje 5 év. Az érvényesség kezdete a kibocsátás ideje. A Titkosító magánkulcsok érvényességi ideje megegyezik a Tanúsítvány érvényességi idejével. Szolgáltató lehetőséget biztosít az előfizetők részére a Tanúsítvány lejártát megelőző 30 napos időszakban arra, hogy a Tanúsítványt megújítsák, a hozzá tartozó kulcspár cseréje mellett.

A megújított Tanúsítvány érvényességének kezdete a megújítás időpontja lesz. Az eredeti Tanúsítvány a megújított Tanúsítvány kibocsátásával egyidejűleg visszavonásra kerül.

Tanúsítvány aktualizálás esetén nem történik kulcscsere. Az új Tanúsítvány a megváltozott adatokat tartalmazza, változatlan érvényességi idővel.

4.8 Katasztrófa elhárítás, szolgáltatói magánkulcs kompromittálódás

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 4.8 fejezetének tartalma érvényes.

5. Fizikai, eljárásrendi, és humán biztonsági szabályozások

Az 5. fejezet bevezető részére a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 5. fejezetének tartalma irányadó, azzal a megjegyzéssel, hogy az ott néhány helyen előforduló, az elektronikus aláírással kapcsolatos kifejezések helyett a megfelelő titkosítási kifejezéseket kell használni.

5.1 Fizikai biztonsági szabályozások

5.1.1 Hitelesítő Központok

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 5.1.1 fejezetének tartalma érvényes.

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 jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 5.2 fejezetének tartalma érvényes.

5.3 Humán szabályozások

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 5.3 fejezetének tartalma érvényes.

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 5.3.1 fejezetének tartalma érvényes.

5.3.2 Biztonsági háttér ellenőrzésekre vonatkozó eljárások

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 5.3.2 fejezetének tartalma érvényes.

5.3.3 A felhatalmazás nélküli tevékenységek büntető következményei

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 5.3.3 fejezetének tartalma érvényes.

5.3.4 A szerződéses alkalmazottakra vonatkozó követelmények

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 5.3.4 fejezetének tartalma érvényes.

5.3.5 A személyzet számára biztosított dokumentációk

A személyzet számára biztosítandó dokumentációt a 9.1 pont sorolja fel.

6. Műszaki biztonsági óvintézkedések

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

Az informatikai rendszer szállítója hitelesítés-szolgáltatási rendszer kiépítésében jelentős tapasztalatokkal rendelkezik, nemzetközileg elismert technológiát alkalmaz.

6.1 Kulcs-pár előállítás és telepítés

6.1.1 Kulcs-pár előállítás

A Szolgáltató maga generálja a kulcspárt biztonságos hardver (HSM) modulban[20], vagy magán a Kulcshordozó kártyán (on-board). Nem fogad el az Előfizető által generált Titkosító magánkulcsot, illetve Kulcshordozó eszközt.

A Szolgáltatónál történő kulcselőállítást fizikailag védett környezetben, bizalmi munkakört betöltő személyzet végzi, legalább kettős ellenőrzés[21] mellett. A kulcspár előállítási funkció végrehajtására felhatalmazott személyzet körét a Szolgáltató, HSzSz-ének megfelelve, a lehető legkisebbre korlátozza. A Szolgáltató a kulcs előállítását a fokozott biztonsági szintnek megfelelő módon állítja elő.

A Titkosító magánkulcs Kulcshordozó eszközön történő elhelyezésére a Szolgáltató csak a hozzá tartozó Tanúsítvány Kulcshordozó eszközön történő elhelyezésével együtt vállalkozik.

A Szolgáltató Kulcshordozó eszközként általában chip kártyát alkalmaz. A chip kártya megszemélyesítés szolgáltatáshoz vizuális – egy oldali nyomással történő – grafikus megszemélyesítése is kapcsolódik az Előfizetői Szerződésben meghatározott adattartalommal. A Kulcshordozó eszköz megszemélyesítése a Szolgáltatónál – fokozott biztonságú környezetben – üzemelő megszemélyesítő rendszeren történik.

A Szolgáltató a Kulcshordozó eszközhöz PIN kódot biztosít.

A generált Titkosító magánkulcs egy példányát a Szolgáltató fokozottan biztonságos körülmények között megőrzi és tárolja (archíválja) a Tanúsítvány érvényességi idejének lejárta, vagy visszavonása után szükségessé váló titkosított állományok visszaállíthatósága céljából.

[20] HSM: Hardware Security Modul
[21] Két személy együttes jelenlétével

6.1.2 A Titkosító magánkulcs Felhasználóhoz történő eljuttatása

A Szolgáltató amikor kulcsokat generál Titkosító magánkulcs felhasználók számára, akkor:

- az általa előállított kulcsokat az Előfizető vagy a Titkosító magánkulcs felhasználó által történő személyes átvételig biztonságos módon tárolja,
- az előállított magánkulcsot a Szolgáltató úgy adja át az Előfizetőnek vagy a Titkosító magánkulcs felhasználónak, hogy a Titkosító magánkulcs titkossága ne sérüljön függetlenül attól, hogy a Kulcshordozó biztonságos chipkártya[22] vagy ettől eltérő, más típusú Kulcshordozó eszköz. Chipkártyától eltérő Kulcshordozó esetén a Titkosító magánkulcsot a transzport nyilvános kulcscsal[23] titkosítva kell a Titkosító magánkulcs felhasználóhoz eljuttatni.
- az átadást követően csak a Titkosító magánkulcs felhasználó férhet hozzá saját magánkulcsához,
- a Szolgáltató biztonságosan ellenőrzi a Kulcshordozó eszköz elkészítését,
- a Szolgáltató a nem megszemélyesített Kulcshordozó eszközt is biztonságosan tárolja,
- a Szolgáltató biztonságosan ellenőrzi a Kulcshordozó eszköz megsemmisítését és újraaktivizálását,
- a Szolgáltató a Kulcshordozó eszköz aktivizálási adatait (PIN kód) biztonságosan készíti el és a Kulcshordozó eszköztől elkülönítve osztja szét.

A Titkosító magánkulcs felhasználóhoz történő eljuttatása a következő két módszerrel juthat el:

- chipkártyás Kulcshordozó alkalmazása esetén a Titkosító magánkulcsot a titkosító hitelesítő központ informatikai rendszeréből a kártyára biztonságos környezetben, zárt folyamatban kell felvinni, kizárva bármely belső munkatárs hozzáférését;

  ezután a kártyát személyesíteni kell, és azt személyesen vagy a megbízott szervezeti képviselő útján a Titkosító magánkulcs felhasználónak át kell adni,

- chipkártyától eltérő Kulcshordozó esetén a Titkosító magánkulcs felhasználó titkosító magánkulcsát a titkosító hitelesítő központ informatikai rendszeréből (a belső titkosítás feloldása után) a Szolgáltató birtokában levő transzport nyilvános kulccsal titkosítva, fájlként kell kiadni az RA munkaállomásra. Ezt a fájlt kell a megbízott kapcsolattartónak a Titkosító magánkulcs felhasználóhoz elvinnie. Ott a kapcsolattartó a Felhasználó által történő PIN

[22] Biztonságos az a kártya, amely nem technológiai sajátosságaiból adódóan teszi lehetővé, hogy a titkosító magánkulcs az első felvitel után hozzáférhető, olvasható, másolható legyen.

[23] A transzport kulcspár azt a célt szolgálja, hogy a Titkosító magánkulcs a hordozóra kerüléstől a Titkosító magánkulcs felhasználó által történő átvételig a transzport nyilvános kulccsal titkosítva kerüljön átvitelre úgy, hogy a transzportáló személy a magánkulcshoz ne férhessen hozzá. A transzportáló személy a Titkosító magánkulcs felhasználó által történő PIN kód megadás után a transzport magánkulccsal állítja vissza a transzportált Titkosító magánkulcsot.

kódos hitelesítés után a transzport magánkulccsal a Felhasználó magánkulcsát a vissza kell állítania és a Felhasználónak át kell adnia. A feloldott titkosító kulcspár PIN kóddal védett PKCS#12 fájlnak kell lennie, így az a kapcsolattartó számára sem közvetlenül hozzáférhető;

a fenti feltételek teljesülése esetén az átadást követően csak a Titkosító magánkulcs felhasználó férhet hozzá saját magánkulcsához,

Az átadás során átadásra kerül:

- Kulcshordozó eszköz és rajta a magánkulcs, illetve a Tanúsítvány
- Az aláírt regisztrációs űrlap egy példánya
- Tájékoztató füzet
- Az aláírt Előfizetői Szerződés egy példánya

A Kulcshordozó eszköz átvételének megtagadása visszavonási kérelemnek számít.

6.1.3 Nyilvános kulcs ellenőrző adat eljuttatása a Tanúsítvány kibocsátóhoz

Az Előfizető titkosító tanúsítványába foglalandó nyilvános kulcsa a Regisztrációs Irodától PKCS#10 tanúsítványigénylés formában, a Regisztrációs Szervezet magánkulcsával elektronikusan aláírt elektronikus üzenetben kerül a Hitelesítő Központhoz.

6.1.4 Hitelesítő Szervezet Aláírás ellenőrző adatának eljuttatása a Felhasználókhoz

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 6.1.4 fejezetének tartalma érvényes.

6.1.5 Kulcs méretek

Az Elsődleges (1. szintű) Hitelesítő Központ ("Root CA")	
aláíró kulcsának mérete:	2048 bit
kommunikációs kulcsának mérete:	1024 bit
A 2. szintű Hitelesítő Központ („Produktív CA”)	
aláíró kulcsainak mérete:	2048 bit
kommunikációs kulcsának mérete:	1024 bit
A Regisztrációs Iroda	
kommunikációs kulcsának mérete:	1024 bit
A Titkosító magánkulcs felhasználók (Előfizetők)	
titkosító magánkulcsainak mérete:	1024 bit

A Szolgáltató folyamatosan figyelemmel kíséri a technikai fejlődést és ennek függvényében szükség esetén gondoskodik kulcshosszak növeléséről.

6.1.6 Előfizetői nyilvános kulcs előállításához használt paraméterek előállítása

A Hitelesítő Központ és a Regisztrációs Iroda az elektronikus aláírás létrehozására az RSA[24] algoritmust használja.

RSA algoritmussal van aláírva a rendszer által kibocsátott minden Tanúsítvány, és ezt az algoritmust használják a rendszeren belül is a letagadhatatlanság (regisztrációs pontokról küldött adatok, tranzakciók aláírása, központi regisztráló szervezet által archivált adatok, tranzakciók) biztosítására.

A Titkosító magánkulcs felhasználók számára kibocsátott tanúsítványok az RSA aláíró algoritmusokhoz használhatók.

A előfizetői nyilvános kulcs generálásához használt paraméterek előállítását a PKI alkalmazás végzi. A szerződéses viszonyban álló Titkosító magánkulcs felhasználók esetében a kulcsgenerálást a Kulcshordozó eszköz on board is elvégezheti.

24 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.

6.1.7 Szoftveres / hardveres kulcsgenerálás

A Szolgáltatóra vonatkozóan biztonságos hardver modulban (HSM) történik a kulcsgenerálás, amelyet a Szolgáltató saját aláírású tanúsítvánnyal hitelesít.

Az előfizetői kulcsokat a Szolgáltató vagy HSM-ben vagy Kulcshordozó eszközön hozza létre.

6.1.8 Kulcs felhasználási célok

A Szolgáltató Előfizető részére kulcspárt a jelen HSzSz hatókörében csak titkosítási céllal bocsát ki.

Ennek érdekében az Előfizetők részére kibocsátott tanúsítványok bővítmény (Extension) részében található „KeyUsage" mezőben a titkosítási célt megjelölő paramétert állít be.

6.2 Magánkulcsok védelme

6.2.1 Kriptográfiai modulra vonatkozó szabványok

Az Előfizetők Titkosító magánkulcsának tárolására Szolgáltató olyan Kulcshordozó eszközt bocsát ki, mely teljesíti a FIPS 140-1 Level 3 követelményeket

A Titkosító magánkulcsot a Szolgáltató PIN kóddal védve bocsátja ki. A Titkosító magánkulcs dokumentált átvétele után az Előfizető felelős a Kulcshordozó eszköz, a Titkosító magánkulcs, valamint a PIN kód védelméért.

A Szolgáltató saját kulcsainak tárolására olyan Kulcshordozó eszközt alkalmaz, amely teljesíti legalább a FIPS 140-1 Level 3 követelményeket.

A Szolgáltató az előfizetői Titkosító magánkulcsokat a Kulcshordozó eszközre a következő módokon viheti fel:

1. Egy olyan biztonságos Kulcshordozó eszközben tárolja, amely nem kompromittálja a magánkulcs biztonságát, megfelel az ISO/IEC 15408 1999/1.,2.,3. szabvány szerint kidolgozott SSCD-PP[25] védelmi profil követelményeinek, és amely szerepel a Nemzeti Hírközlési Hatóság elektronikus aláírás termék listáján.

[25] A védelmi profil pontos megnevezése: Protection Profile – Secure Signature-Creation Device Type 2, verzió száma: 1.05, regisztrációs száma: BSI-PP-0005-2002, értékelés garancia szintje: emelt EAL4

2. A Titkosító magánkulcs a 6.1.2 pontban meghatározott módon a transzport nyilvános kulccsal titkosítva kerül a Kulcshordozó eszközre, amelyet a megbízott kapcsolattartó a 6.1.2 pontban meghatározott módon állít vissza Titkosító magánkulcs felhasználó jelenlétében.

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

A Szolgáltatónál egyedül a Hitelesítő Központban alkalmazzák az „n-ből m" ellenőrzést.

6.2.3 Titkosító magánkulcs letét

A Szolgáltató az előfizetői titkosító magánkulcsokat megbízható és biztonságos körülmények között tárolja, annak érdekében, hogy szükség esetén a magánkulcs érvényességi idejének lejárta vagy visszavonása esetén a korábban titkosított állományok visszaállíthatók legyenek.

Az előfizetői titkosító magánkulcsot a Szolgáltató letétbe nem helyezheti.

6.2.4 Titkosító magánkulcs mentése

A Szolgáltató a titkosító kulcsokat generálás után megbízható és biztonságos körülmények között tárolja, annak érdekében, hogy szükség esetén a magánkulcs érvényességi idejének lejárta vagy visszavonása esetén a korábban titkosított állományok visszaállíthatók legyenek.

Szolgáltató az előfizetők Titkosító magánkulcsait csak archiválási céllal menti.

6.2.5 Titkosító magánkulcs archiválása

A Szolgáltató az előfizetői titkosító magánkulcsokat az egyéb adatok archiválási módjától elkülönülten, fokozottan biztonságos körülmények között tárolja.

6.2.6 Magánkulcsok kriptográfiai modulba helyezése

A Hitelesítő és Regisztráló szervezetekre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 6.2.6 pontja irányadó.

A végfelhasználókra vonatkozóan lásd a 6.1.1 és a 6.1.2 pontban a végfelhasználókra vonatkozó részt!

6.2.7 Magánkulcsok aktiválása

Az előfizetői Titkosító magánkulcs aktiválása a Felhasználó által történik a jelszó vagy PIN kód megadásával, azokban az esetekben, amikor a Titkosító magánkulcs használatára szükség van.

A Kulcshordozó eszközt a Titkosító magánkulcs aktiváláskor sem hagyja el, azt az eszközről leolvasni nem lehet.

6.2.8 Magánkulcsok deaktiválása

Az előfizetői Titkosító magánkulcsok deaktiválását a Felhasználó alkalmazása végzi a Titkosító magánkulcs felhasználó kijelentkezésekor, vagy amikor a Titkosító magánkulcs felhasználó a Kulcshordozó eszközt eltávolítja az olvasóból.

6.2.9 Magánkulcsok megsemmisítése

Az előfizetői Titkosító magánkulcs lejárta után a Kulcshordozó eszköz fizikai megsemmisítését az Előfizetőnek saját felelősségi körében úgy kell elvégezni, hogy az semmilyen körülmények között ne legyen újra felhasználható.

A szolgáltatói Titkosító magánkulcsok megsemmisítése a Szolgáltató kötelessége.

6.3 Kulcs-pár kezelés egyéb aspektusai

6.3.1 Nyilvános kulcsok archiválása

Az előfizetői tanúsítványokat a nyilvános kulcsokkal együtt Szolgáltató az érvényesség lejáratától számított 10 évig archiválja. Az archív adatállományt Szolgáltató az erre a célra létrehozott Aláírás létrehozó adatával aláírja, s legalább két példányban menti.

Az adathordozók egyik példányát Szolgáltató a Hitelesítő Központjában, a másik példányát a földrajzilag távol eső Biztonsági Adattárában tárolja a megőrzési idő végéig.

6.3.2 Tanúsítványok felhasználási ideje

A Root CA aláíró kulcshoz tartozó Tanúsítvány érvényességi ideje:	10 év
A Produktív CA aláíró kulcsához tartozó Tanúsítvány érvényességi ideje:	legfeljebb 10 év
Az RO kommunikációs kulcsához tartozó Tanúsítvány érvényességi ideje:	legfeljebb 3 év
Az Előfizető titkosító kulcsához tartozó Tanúsítvány érvényességi ideje:	5 év
A transzport Tanúsítvány érvényességi ideje:	tetszőleges

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 által kibocsátott Kulcshordozó eszközök aktivizáló adatait (PIN kódjait) a PKI alkalmazás állítja elő.

6.4.2 Aktiválási adatok védelme

A Regisztrációs Iroda az általa kibocsátott Kulcshordozó eszközök aktivizáló adatait (PIN kódjait) műszaki[26] és szervezési[27] intézkedésekkel védi, majd a Kulcshordozó eszköztől elkülönítve[28] osztja szét.

A Titkosító magánkulcsnak a Felhasználó által történő birtoklása az alapvető feltétel a titkosított állomány visszaállíthatóságának biztosítására. Emiatt a Felhasználónak saját felelősségi körében kell biztosítania a kizárólagos birtoklást. Amennyiben ez sérül vagy elvszik, illetve ennek alapos gyanúja fennáll, akkor a Felhasználónak ezt haladéktalanul jelentenie kell az őt regisztráló Irodánál, illetve jogi személy esetén a megbízott kapcsolattartónál, amely/aki azonnal intézkedik a Tanúsítvány visszavonásáról.

A Felhasználó Titkosító magánkulcsának aktiválási adatát (PIN) kódját a Szolgáltató a Titkosító magánkulcs előállítása után megsemmisíti, büntetőjogi felelőssége mellett nem hozza harmadik fél tudomására.

A Felhasználó bármikor megváltoztathatja a jelszavát vagy PIN kódját.

A Szolgáltató a saját aktiválási adatait a MeH 12. ajánlás által meghatározott fokozott biztonsági szinten védi a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz 2.8 fejezetében (Bizalmasság – Adatkezelési szabályzat), a 4.5 fejezetében (Biztonsági audit

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

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

eljárások), az 5. fejezetében (Fizikai, eljárásrendi, és humán biztonsági szabályozások), és a 6.5 fejezetében (Számítógép biztonsági szabályok) meghatározott biztonsági intézkedésekkel.

6.4.3 Aktiválási adatok egyéb aspektusai

Az Felhasználó 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 aktiválási adatot kell előállítani.

6.5 Számítógép biztonsági szabályok

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 6.5 fejezetének tartalma érvényes.

6.6 Életciklus technikai szabályok

6.6.1 Rendszerfejlesztési szabályok

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 6.6.1 fejezetének tartalma érvényes.

6.6.2 Biztonságkezelési szabályok

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 6.6.2 fejezetének tartalma érvényes.

6.7 Hálózati biztonsági szabályok

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 6.7 fejezetének tartalma érvényes.

6.8 Kriptográfiai modul ellenőrzése

A titkosítás-hitelesítést támogató informatikai rendszerben működő kriptográfiai modul ellenőrzi az illetéktelen beavatkozási kísérleteket.

---

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

Amennyiben ilyet detektál, akkor:

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

borítékokban történik.

7. Tanúsítvány és kulcs-visszavonási profil

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 7. fejezetének tartalma érvényes, azzal a kiegészítéssel, hogy a Tanúsítvány „*Kulcshasználat*” kiterjesztési mezejében a titkosításra utaló paramétert be kell jelölni, valamint Policy OID-ként a Titkosító Tanúsítványokra érvényes 1.2 pont szerinti OID-t kell megadni.

8. HSzSz adminisztráció

A jelen fejezetre a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz aktuális változata 8. fejezetének tartalma érvényes.

9. Hivatkozások és meghatározások

9.1 Hivatkozások

Hivatkozott törvények, kormányrendeletek, MeH rendeletek:

- 2001. évi XXXV. törvény az elektronikus aláírásról,
- 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról,
- 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról,
- 1995. évi CXXII. törvény a polgárok személyes adatainak nyilvántartásáról szóló 1992. évi LXVI. törvény módosításáról szóló törvény.

A Szolgáltató hivatkozott dokumentumai:

- 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
- Hitelesítési Politika Nem Minősített Tanúsítványtípusokra (HP)
- Hitelesítés Szolgáltatási Szabályzat a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatáshoz (a Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatásra érvényes HSzSz)
- Általános Szerződési Feltételek Fokozott Biztonságú Hitelesítés Szolgáltatáshoz (ÁSzF)
- Előfizetői Szerződés Minta
- A Trust&Sign Szolgáltatások Biztonságpolitikája
- A Trust&Sign Szolgáltatások Biztonsági Szabályzata
- A Trust&Sign Szolgáltatások Üzletmenet-folytonossági Terve
- A Trust&Sign Szolgáltatások 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 2459 és RFC 2527 ajánlásai,
- Európai Unió ETSI TS 101 456 és ETSI TS 101 862 szabványai,

- NIST FIPS 140-1 Level 1-3,
- a CWA 14167-1, és a CWA 14172-1,-2,-3,-4 CEN Workshop Agreement-ek
- MeH 12. ajánlás,
- ITSEC, Common Criteria.

9.2 Meghatározások

Biztonságos kulcshordozó eszköz: Az elektronikus aláírás törvény 1. számú mellékletében foglalt követelményeknek eleget tevő Kulcshordozó eszköz.

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

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

Címtár szolgáltatások: A hitelesítő szervezet a regisztráló szervezeten keresztül fogadja és feldolgozza a Tanúsítványokkal kapcsolatos változások adatait, nyilvántartást vezet a Tanúsítványok aktuális helyzetéről, esetleges felfüggesztéséről, illetve visszavonásáról. Ezeket az információkat, valamint a Tanúsítványokhoz tartozó nyilvános (aláíró és titkosító) kulcsokat, továbbá a visszavont Tanúsítványok nyilvántartását (CRL) Internet segítségével bárki számára hozzáférhető és folyamatosan elérhető módon közzéteszi a Tanúsítványtárban.

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

Elektronikus dokumentum: elektronikus eszköz útján értelmezhető adategyüttes.

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.

Érvényességi lánc: az elektronikus dokumentum vagy annak lenyomata, és azon egymáshoz rendelhető információk sorozata, amely alapján megállapítható, hogy az elektronikus dokumentumon elhelyezett fokozott biztonságú vagy minősített aláírás, illetve időbélyegző, valamint az azokhoz kapcsolódó tanúsítványok az aláírás és időbélyegző elhelyezésének időpontjában érvényes volt.

Ellenőrzési lépések: A Titkosító nyilvános kulccsal történő titkosításkor a Titkosító magánkulcs felhasználó Tanúsítványa ellenőrzésekor kötelezően elvégzendő műveletsor.

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

Érintett fél: Az elektronikus állomány tikosítását végző entitás (személy/eszköz), aki/amely a Titkosító magánkulcs felhasználó Nyilvános kulcsához tartozó Tanúsítvány ellenőrzése alapján kezdeményezi az elektronikus állomány titkosítását.

Fokozott biztonságú szolgáltató: a Nemzeti Hírközlési Hatóságnál bejelentett és nyilvántartási számmal rendelkező (regisztrált) elektronikus aláírás-hitelesítés szolgáltató, amely a 2001. évi XXXV. törvényben és a 151/2001. (IX. 1.) Korm. rendeletben foglaltaknak megfelel és az elektronikus aláírás-hitelesítés szolgáltatás mellett fokozott biztonságú Titkosító kulcspárt és ehhez tartozó Tanúsítványt bocsát ki.

Hitelesítő szervezet (CA): a Hitelesítés Szolgáltató azon egysége, amely a hitelesítés-szolgáltatás hitelesítő kulccsal folytatott tevékenységét végzi. A központ fizikailag egy telephelyre koncentráltan, védett, biztonságos körülmények között működik.

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

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

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

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

Kompromittálódás: Az az eset, amikor a Kulcshordozó eszköz használatára, illetve a Kulcshordozó eszköz eredeti tulajdonosának küldött titkosított elektronikus állományok visszaállítására arra nem jogosított személy képessé válik.

(Kriptográfiai) Kulcs: Kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete a titkosításhoz, illetve a titkosított állomány visszaállításához szükséges.

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

Kulcshordozó eszköz: Szoftver vagy hardver, melynek segítségével a Titkosító magánkulcs felhasználó a Titkosító magánkulcsának felhasználásával a titkosított elektronikus állományt visszaállítja.

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

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

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

Regisztráló szervezet: A regisztráló szervezetek a Szolgáltató és a vele szerződése alapon együtt működő Társaságok azon szervezeti egységei, amelyek az előfizetők adatainak regisztrációját, ellenőrzését, az igénylő személyazonosságának és hitelességének megállapítását, a Tanúsítvány kérelmek összeállítását, a hitelesítő szervezethez történő továbbítását, és egyéb azonosítási, Tanúsítványmenedzsment és adminisztrációs feladatokat látnak el a HP-ben és az Általános Szolgáltatási Feltételekben előírtak szerint. Az aktuális listát lásd a *http://www.mavinformatika.hu/ca* weboldalon.

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

Szolgáltatás: Elektronikus Titkosító tanúsítvány hitelesítés-szolgáltatás (röviden: hitelesítés-szolgáltatás) és Titkosító magánkulcs előállítása és elhelyezése a Titkosító magánkulcsot tároló eszközön.

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

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

Tanúsítvány: A hitelesítés szolgáltató által kibocsátott igazolás, amely a Nyilvános kulcsot az elektronikus aláírásról szóló törvény szerint egy meghatározott személyéhez kapcsolja és igazolja e személy személyazonosságát vagy valamely más tény fennállását, ideértve a hatósági (hivatali) jelleget.

Tanúsítvány frissítés: amikor a hitelesítés-szolgáltató érvényes magánkulcsával az új Tanúsítványban a Tanúsítvány alanyának változatlan (régi) Nyilvános kulcsát és változatlan egyéb adatait írja alá új érvényességi időtartamra,

Tanúsítvány aktualizálás: amikor a hitelesítés-szolgáltató érvényes magánkulcsával az új Tanúsítványban a Tanúsítvány alanyának változatlan (régi) Nyilvános kulcsát és megváltozott új adatait írja alá új érvényességi időtartamra,

Tanúsítvány kulcscsere: amikor a hitelesítés-szolgáltató érvényes magánkulcsával az új Tanúsítványban a Tanúsítvány alanyának új Nyilvános kulcsát és változatlan egyéb adatait írja alá új érvényességi időtartamra.

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

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

Titkosító magánkulcs: Olyan egyedi adat (jellemzően kriptográfiai magánkulcs), amellyel a Titkosító magánkulcs felhasználó a az Érintett fél által küldött, titkosított elektronikus állományt visszaállítja a titkosítás előtti tartalomra.

Titkosító magánkulcs felhasználó: Egy Tanúsítványban azonosított entitás, aki a Tanúsítványban szereplő Nyilvános kulcsnak megfelelő magánkulcsot birtokolja.

Titkosító nyilvános kulcs: Olyan egyedi adat (jellemzően kriptográfiai Nyilvános kulcs), amellyel az Érintett fél az elektronikus állományt titkosítja.

Titkosító tanúsítvány: olyan, az RFC 2527 szabványban leírt X.509 3-as verziójú Tanúsítvány, amelyben a kulcshasználat titkosításra van beállítva.

Transzport kulcspár: A transzport kulcspár azt a célt szolgálja, hogy a Titkosító magánkulcs a hordozóra kerüléstől a megbízott kapcsolattartó által történő transzporton keresztül a Titkosító magánkulcs felhasználó által történő átvételig a transzport nyilvános kulccsal titkosítva kerüljön átvitelre úgy, hogy a transzportáló személy a magánkulcshoz ne férhessen hozzá. A transzportáló személy a Titkosító magánkulcs felhasználó által történő PIN kód megadás után a transzport magánkulccsal állítja vissza a transzportált Titkosító magánkulcsot.

Transzport tanúsítvány: A transzport kulcspárhoz tartozó Tanúsítvány.

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.