MÁV INFORMATIKA

Kereskedelmi, Szolgáltató és Tanácsadó Korlátolt Felelősségű Társaság

Szolgáltatási Szabályzat a minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz (HSZSZ-M)

Verziószám	**4.0**
OID szám	**1.3.6.1.4.1.14868.1.2.4**
Hatósági nyilvántartásba vétel napja	**2006. május 22.**
Hatósági nyilvántartásba vétel száma	**HL 8715-3/2006.**
Hatálybalépés dátuma	**2006. május 22.**

1012 Budapest, Krisztina krt. 37/a. 1253 Budapest Pf. 28. Tel.: 457-9200, fax: 457-9500, e-mail: mavinformatika@mavinformatika.hu

HSZSZ-M verziók

Verzió	Dátum	A változás leírása	Készítette
1.0	2002.09.30	A fokozott biztonságú szolgáltatói regisztrálásra előkészített, a HIF részére átadott változat.	Bodlaki Ákos
2.0	2002.11.29	HSZSZ-M minősített tanúsítványtípusokra, véleményezésre átadott változat	Bodlaki Ákos
2.1	2003.03.31.	A minősítési eljárásra átadott változat kiegészítve és módosítva a HIF észrevételeivel	Bodlaki Ákos
2.2	2003.07.30	Időbélyegzés szolgáltatás minősítési eljárására beadott 1.0 változattal kapcsolatos észrevételekkel módosítva.	Bodlaki Ákos
2.2.1	2004. 01. 20.	Formai és sajtóhibák javítása, belső ellentmondások megszűntetése szakértői észrevételek alapján. Felülvizsgált és javított változat	Néder Ferenc
2.3	2004. 08. 23.	A 2004. évi LV. törvény hatásainak átvezetése	Néder Ferenc
3.0	2005. 07. 21.	Felülvizsgált, OCSP[1]-vel bővített változat	Néder Ferenc
4.0	2006. 04. 13.	Felülvizsgált, az NHH észrevételei alapján javított, a 2004. évi CXL. törvény (a közigazgatási hatósági eljárás és szolgáltatás általános szabályai) előírásainak megfelelő változat	Néder Ferenc

[1] OCSP: On-line Certificate Status Protocol, magyarul: valós idejű tanúsítvány-állapot lista

TARTALOMJEGYZÉK

1.Bevezetés

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

A Szolgáltató szolgáltatásait a vele előfizetői szerződéses viszonyban álló *Előfizetők* és az elektronikus aláírások hitelességét ellenőrző *érintett felek* részére nyújtja.

A minősített elektronikus aláírással kapcsolatos szolgáltatások (továbbiakban: szolgáltatások) keretében a Szolgáltató a 2001. évi XXXV. törvényben meghatározott szolgáltatások közül a következőket nyújtja:

a. elektronikus aláírás hitelesítés-szolgáltatás (a továbbiakban: hitelesítés-szolgáltatás)

b. aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése

c. időbélyegzés

A HSZSZ-M további fejezeteiben a „*szolgáltatások*” kifejezés alatt a fenti részszolgáltatások bármelyike, vagy azok kombinációja értendő.

A szolgáltatások részletezése az 1.4.4.2 pontban olvasható.

1.1. Szolgáltató adatai

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

Cégjegyzék szám: 01-09-563711

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

Telefonszám: (36-1) 457-9300

Telefax szám: (36-1) 457-9500

Internetes honlap címe: *http://www.mavinformatika.hu/*

Szolgáltatás internetes honlapjának címe: *http://www.mavinformatika.hu/ca/*

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:

Az ügyfélkapcsolatok (általános és részletes tájékozódás, szerződéskötés, aláírás létrehozó eszköz átadása, visszavonási kérelem megerősítése, stb.) biztosítása érdekében a Szolgáltató Ügyfélkapcsolati Irodákat tart fenn, melyeket az ügyfelek személyesen azok nyitvatartási idejében kereshetnek fel. A mindenkori nyitvatartási rendeket a Szolgáltató a Szolgáltatás honlapján teszi közzé.

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

A központi 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 a *hiteles@mavinformatika.hu* címen.

A területi ügyfélkapcsolati irodák címe és elérhetősége a Szolgáltatás Internetes honlapján keresztül érhető el.

A tanúsítványok felfüggesztésére a Szolgáltató folyamatos (7x24 órás) ügyfélszolgálatot (Help Desk szolgálatot) ad. Az Ügyfélszolgálat elérhető a +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.

Panaszok bejelentésének helye:

a. személyesen az Ügyfélkapcsolati Irodákban

b. írásban a Szolgáltató székhelyére címezve

c. telefonon az Ügyfélkapcsolati Irodákban vagy az Ügyfélszolgálatnál

d. elektronikus levélben a *mavinformatika@mavinformatika.hu* és az *hiteles@mavinformatika.hu* címeken

1.2. Alapok

1.2.1. Szabályzat célja

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

1.2.2. Jogszabályok, szabványok

A jelen HSZSZ-M a következő jogszabályokat, szabványokat és ajánlásokat veszi figyelembe a HSZSZ-M teljes tartalmára vonatkozóan:

- 2001. évi XXXV. törvény az elektronikus aláírásról (a továbbiakban: Eat.),
- 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól (a továbbiakban: Ket.)
- 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- ISO/IEC 15408 1999: Információ technológia - Biztonsági módszerek - Informatikai biztonság értékelési kritériumai (1-3 részek)

A HSZSZ-M szerkezetére és tartalmára vonatkozóan:

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

A minősített tanúsítványok, visszavonási listák szerkezetére és tartalmára vonatkozóan:

- International Telecommunication Union X.509 “Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer”
- Minősített tanúsítványtípus minták minősített hitelesítés-szolgáltatók számára, 1.0 verzió. Hírközlési Felügyelet.
- ETSI TS 101 862 Minősített tanúsítvány profil
- RFC 2459 illetve RFC 3280 (Internet X.509 Nyilvános kulcsú infrastruktúra – Tanúsítvány és Tanúsítvány visszavonási lista profil)
- ITU-T X.509 “Information technology - Open Systems Interconnection - The Directory: Public -key and attribute certificate frameworks” ajánlás 3. verziója,
- RFC 3039 (Internet X.509 Nyilvános kulcsú infrastruktúra – Minősített tanúsítvány profil)
- ISO 3166 szabvány

A minősített hitelesítés-szolgáltatókra vonatkozóan:

- 194/2005. (IX. 22.) Korm. rendelet a közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítés-szolgáltatókra vonatkozó követelményekről
- 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- 45/2005. (III. 11.) Korm. rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól
- 2/2002. (IV. 26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről,
- ETSI TS 101 456 (Minősített tanúsítványokat kibocsátó hitelesítés-szolgáltatókra vonatkozó szabályozási követelmények).

Az időbélyegzésre vonatkozóan:

RFC – 3161 (Internet X. 509 nyilvános kulcsú infrastruktúra időbélyeg protokoll)

ETSI TS 102 023 (2003. 04) (Időbélyegzés szolgáltatókra vonatkozó követelmények)

ETSI TS 101 861 szabvány (Időbélyegzés profil)

Az OCSP szolgáltatásra vonatkozóan:

IETF RFC 2560 szabvány

Az informatikai biztonsági követelményekre vonatkozóan:

MeH ITB 12. ajánlás, ITSEC[2], CC[3]

A kriptográfiai modulra, az aláírás-létrehozó eszközre vonatkozóan:

NIST FIPS PUB 140-1 (1994. január 11.) (Kriptográfiai modulok biztonsági követelményei),

ITSEC, CC,

CEN 14167-2 munkacsoport egyezmény: „Védelmi profil hitelesítés-szolgáltató aláíró műveleteit megvalósító kriptográfiai modulra" (MCSO-PP, HSM-PP),

CEN 14167-3 munkacsoport egyezmény: „Védelmi profil hitelesítés-szolgáltató kulcs előállítási szolgáltatásait megvalósító kriptográfiai modulra" (CMCKG-PP, HSM-PP)

CWA 14167-1, és a CWA 14172-1,-2,-3,-4 CEN Workshop Agreement-ek

1.3. HSZSZ-M azonosítás

A Szolgáltató az ISO/IEC és az ITU szabványok által előírt regisztrációs eljárásoknak megfelelően azonosítja a jelen HSZSZ-M-t.

A dokumentum neve:	Szolgáltatási Szabályzat a minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz. A jelen dokumentumban és a kapcsolódó szabályzatokban HSZSZ-M-ként történik rá hivatkozás.
PKI szoftver technikai azonosító:	T&S QCAV1.0
Időbélyegző szoftver technikai azonosító:	T&S TSAV1.0
Első hatálybalépés időpontja	2003. április 3.

A HSZSZ-M jelen aktuális verziója a PKI alkalmazás mindenkori technikai azonosítójával van összerendelve, azaz a HSZSZ-M-ben foglaltak a technikai azonosítóval azonosított PKI alkalmazásra vonatkoznak.

A szabályzat vonatkozó pontjai tartalmazzák az időbélyegzés szolgáltatásra vonatkozó gyakorlati szabályokat és megoldásokat, amelyek az Időbélyegzés Szolgáltatási Rend (továbbiakban: ISZR) szerint lettek kialakítva.

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

1.4. Hitelesítés szolgáltató és felhasználói közösség, alkalmazhatóság

A Szolgáltató által kibocsátott tanúsítványokat felhasználó közösség a következő:

a. a Szolgáltató regisztráló és hitelesítő egységei, a szolgáltatást működtető elektronikus aláírásra feljogosított munkatársai

b. az Előfizetők és az Aláírók

c. az Előfizetők és az Aláírók informatikai eszközei (szerverek, kommunikációs kapcsolatok, alkalmazások, stb.)

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

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

d. az érintett felek

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

a. az Előfizetők
b. az időbélyegzés szolgáltató
c. az időbélyeget felhasználó (igénybevevő) fél
d. az érintett felek

Az időbélyegzés szolgáltatást minden, az ISZR 4.3 pontban meghatározott időbélyeg felhasználó igénybe veheti, függetlenül attól, hogy az időbélyeget nyilvános vagy zárt körben használja.

OCSP vonatkozásában a közösséget az ISZR 4. pontjában meghatározott, következő csoportok alkotják:

a. az Előfizetők
b. az OCSP szolgáltató
c. az OCSP válaszokat felhasználó (igénybevevő[4]) fél
d. az érintett felek

1.4.1. A Szolgáltató regisztráló és hitelesítő egységei

A Szolgáltató minősített hitelesítés-szolgáltató.

A Szolgáltató regisztráló és hitelesítő egységei:

Az Ügyfélkapcsolati Irodák, melyek elvégzik az igénylők (a későbbi Előfizetők) adatainak felvételét, az Előfizető személyazonosságának megállapítását, a tanúsítvány kérelmek összeállítását és gondoskodnak az előfizetői szerződésben foglaltak teljesítéséről.

A Regisztrációs Iroda, mely a szolgáltatás keretein belül biztosítja az Előfizetők technikai regisztrációját, a tanúsítványok felfüggesztés és visszavonás kezelését és az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezését.

A Szolgáltató Hitelesítő Központja, amely a szolgáltatás-támogató informatikai rendszer központi erőforrásaiból, azt ezt körülvevő biztonságos fizikai környezetből valamint az üzemeltetést és szolgáltatást ellátó személyzetből áll.

A Szolgáltató regisztráló és hitelesítő egységei részletes feladat és felelősségi körét a HSZSZ-M 2.1.1 pontja írja le.

1.4.2. Előfizetők és Aláírók (felhasználók, alanyok)

Előfizető a Szolgáltatóval szerződéses viszonyban álló felhasználó, aki számára a Szolgáltató tanúsítványt és/vagy időbélyeget bocsát ki. Előfizető lehet természetes vagy jogi személy.

Aláíró (alany) az a természetes személy, aki az aláírás-létrehozó eszközt birtokolja és a saját vagy más személy nevében aláírásra jogosult.

Az Előfizető lehet egyben Aláíró is, ha saját maga birtokolja és használja az aláírás-létrehozó eszközt.

1.4.3. Érintett felek

Az Érintett fél (aláírás Ellenőrző) olyan természetes vagy jogi személy, aki vagy amely, az aláírt és/vagy időbélyegzett és/vagy OCSP válasszal ellátott elektronikus dokumentum fogadója, és egy adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el az aláírás, és/vagy az időbélyeg és/vagy az OCSP válasz hitelességének ellenőrzésekor.

1.4.4. Alkalmazhatóság

1.4.4.1. Szabályzat hatálya

A HSZSZ-M időbeli hatálya a hatálybalépés dátumával kezdődik és határozatlan időre szól. Időbeli hatálya megszűnik a szolgáltatási tevékenység beszüntetésekor, illetve egy újabb szabályzat verzió hatályba lépésével.

A HSZSZ-M személyi hatálya a szolgáltatóra, annak a szolgáltatásban közreműködő munkatársaira és a felhasználói közösségre terjed ki.

A HSZSZ-M tárgyi hatálya a következőkre terjed ki:

a. az 1. pontban meghatározott szolgáltatásokra
b. a Szolgáltatónak a hitelesítés szolgáltatással kapcsolatban álló összes objektumára és tárgyi eszközére

[4] Igénybevevő: az OCSP kérést elindító és a választ fogadó felhasználó

1.4.4.2.Szolgáltatás szintje

A Szolgáltató az Eat. szerinti minősített szolgáltatásokat nyújtja, melyek az alábbi összetevőkből épülnek fel:

a. Tanúsítvány kialakítási szolgáltatás, ebben regisztráló szolgáltatás és egyedi-név szolgáltatás, valamint megszemélyesítési szolgáltatás

b. Tanúsítvány kiadás és tanúsítvány szétosztási szolgáltatás

c. Felfüggesztési és visszavonás kezelési szolgáltatás

d. Tanúsítvány megújítási szolgáltatás

e. Biztonságos aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése

f. Biztonságos aláírás-létrehozó eszköz fizikai megszemélyesítése (arculati elemek elhelyezése az eszközön)

g. Időbélyegzés

h. OCSP szolgáltatás

1.4.4.3.Tanúsítványok alkalmazhatósága

Az előfizetői tanúsítványok alkalmazhatóságára a következő alapszabályok érvényesek:

Engedélyezett alkalmazási lehetőségek

A kibocsátott magánkulcsok (aláírás-létrehozó adatok) kizárólag elektronikus aláírások megtételére használhatók. A magánkulcsokhoz tartozó nyilvános kulcsok (aláírás-ellenőrző adatok) az elektronikus aláírások ellenőrzésére használhatók fel.

Korlátozott alkalmazási lehetőségek

Szolgáltató területi, pénzügyi, stb. korlátozásokat szabhat saját belső hitelesítési rendje szerint, amelyeket a kibocsátott előfizetői tanúsítványban megad.

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

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, amely támogatja a PKI technológián alapuló elektronikus aláírási, le nem tagadhatósági funkciókat. A Szolgáltató nem vállal felelősséget az elektronikus aláírásra kibocsátott aláírás-ellenőrző adat, illetve a titkosításra, vagy más, az elektronikus aláírástól eltérő felhasználására vonatkozóan.

A 2/2002. (IV.26) MeHVM irányelve 214. pontja értelmében az időbélyegzéshez kibocsátott tanúsítványokat, illetve aláíró kulcsokat kizárólag a Szolgáltató által létrehozott időbélyegek aláírására lehet használni.

Jelen HSZSZ-M hatálya alatt kibocsátott tanúsítványok csak az 1.4 fejezetben meghatározott hitelesítés-szolgáltató és felhasználó közösség körében használhatók az Előfizetői Szerződésben meghatározott összeghatárok szerinti korlátokkal, betartva a tanúsítványokban található esetleges egyéb korlátozásokat is.

A tanúsítvány használati lehetőségére vonatkozó fenti információk a tanúsítványban is rögzítésre kerülnek. A tanúsítvány használati lehetőségére vonatkozó információktól bármely módon eltérő használat az Aláíró egyéni felelőssége és kockázata, ahogy az ilyen módon felhasznált tanúsítvány elfogadása az érintett fél (aláírás Ellenőrző) felelőssége és kockázata.

1.5. Tanúsítvány osztályok, tanúsítványtípusok és tanúsítvány fajták

A jelen HSZSZ-M a nyilvános körben kibocsátott minősített tanúsítványokat és az ezzel kapcsolatos szabályokat írja le.

A minősített tanúsítványok bizalmi osztályába két tanúsítványtípus tartozik:

a. nyilvános körben kibocsátott minősített tanúsítványtípus (MTT)

b. nyilvános körben kibocsátott és biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített tanúsítványtípus (MTT+BALE)

Kötelezettség vállalással csak Előfizetői tanúsítvány adható ki. A kötelezettségvállalás értékhatárát az Előfizetői Szerződés rögzíti és ezt az értékhatárt a Szolgáltató a tanúsítványban feltünteti.

Szolgáltató által kibocsátott Előfizetői tanúsítványok érvényességi ideje legfeljebb 1 év. Az érvényesség kezdete a kibocsátás napja. Az előfizetői tanúsítványok érvényessége az érvényességi idő lejárata előtt legfeljebb egy alkalommal legfeljebb egy évre meghosszabbítható (lásd: 4.6 - 4.9 pontok).

1.5.1. Minősített tanúsítványok jellemzői és típusai

1.5.1.1. Minősített tanúsítványok jellemzői

Minősített tanúsítvány az Eat. 2. számú mellékletében foglalt követelményeknek megfelelő olyan tanúsítvány, amelyet minősített szolgáltató bocsátott ki. A minősített tanúsítványoknak tartalmazniuk kell az alábbiakat:

a. annak megjelölését, hogy a tanúsítvány minősített tanúsítvány
b. a Szolgáltató és székhelyének (ország-) azonosítóját
c. az Aláíró nevét (vagy egy álnevét, ennek jelzésével)
d. a tanúsítvány szándékolt felhasználásától függően az Aláíró külön jogszabályban, a jelen Szolgáltatási Szabályzatban és az Általános Szerződési Feltételekben (továbbiakban: ÁSZF-M-ben) meghatározott speciális jellemzőit
e. az Aláíró által birtokolt aláírás-létrehozó adatnak megfelelő aláírás-ellenőrző adatot
f. a tanúsítvány érvényességi idejének kezdetét és végét, valamint azt az időtartamot, ameddig a Szolgáltató az Eat. 9. § (7) bekezdés szerinti feladatokat ellátja
g. a tanúsítvány azonosító kódját
h. a tanúsítványt kibocsátó Szolgáltató fokozott biztonságú elektronikus aláírását
i. a tanúsítvány használhatósági körére vonatkozó esetleges korlátozásokat
j. a tanúsítvány felhasználásának korlátjait, (beleértve a kötelezettségvállalás korlátait is)
k. szervezet képviseletére jogosító elektronikus aláírás tanúsítványa esetén a tanúsítvány ezen minőségét és a képviselt szervezet azonosító adatait.

1.5.1.2. Nyilvános körben kibocsátott minősített tanúsítványtípus (MTT)

Az MTT olyan tanúsítványtípus, amely:

a. megfelel az Eat. 2. számú mellékletében meghatározott követelményeknek
b. olyan Szolgáltató adta ki, amely teljesíti az Eat. 3. számú mellékletében meghatározott követelményeket
c. nyilvános körben került kibocsátásra

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

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

Az MTT+BALE olyan tanúsítványtípus, amely:

a. megfelel az Eat. 2. számú mellékletében meghatározott követelményeknek
b. olyan Szolgáltató adta ki, amely teljesíti az Eat. 3. számú mellékletében meghatározott követelményeket
c. olyan biztonságos aláírás-létrehozó eszköz került felhasználásra, amely eleget tesz az Eat. 1. számú mellékletében meghatározott követelményeknek
d. nyilvános körben került kibocsátásra.

A minősített tanúsítványok olyan elektronikus aláírások igazolására használhatók, amelyek az aláírás jogi követelményeit az elektronikus formájú adatok vonatkozásában ugyanolyan módon kielégítik, mint egy kézírásos aláírás a papír-alapú adatok vonatkozásában. Az ilyen körülmények között készített elektronikus aláírást ***minősített elektronikus aláírás***-nak kell tekinteni.

1.5.2. Tanúsítványok használati osztályainak jellemzői

1.5.2.1. Előfizetői tanúsítvány

Előfizetői tanúsítvány a Szolgáltatóval szerződéses viszonyban álló Előfizető számára kibocsátott tanúsítvány.

Az Előfizetői tanúsítványok objektum-azonosítója (OID): 1.3.6.1.4.1.14868.2.2.1 (MTT)

1.3.6.1.4.1.14868.2.2.2 (MTT+BALE)

0.2.216.1.100.42.101.1.2.1 [MHR_Ü]

0.2.216.1.100.42.101.2.2.1 [MHR_K]

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

Ha az Aláíró természetes személy bármely más természetes vagy jogi személyt képvisel, akkor a képviseleti jogot írásos megbízói nyilatkozattal kell igazolni. Ebben az esetben az Aláírók hiteles személyazonosságának megállapításáról a Szolgáltató közjegyzői okiratot is elfogad.

1.5.2.2.Szolgáltatói tanúsítvány

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

A Szolgáltatói tanúsítványok objektum-azonosítója (OID): 1.3.6.1.4.1.14868.2.1.1

1.5.3.Tanúsítvány fajták és tulajdonságaik

A Szolgáltató a következőkben meghatározott fajtájú minősített tanúsítványokat adhatja ki Előfizetők részére, illetve saját céljaira.

1.5.3.1.„Személyes” tanúsítvány

„Személyes” típusú tanúsítványt európai uniós állampolgárságú természetes személy igényelhet a saját nevében. A személyes típusú tanúsítvány esetében az Előfizető és az Aláíró jellemzően ugyanaz a személy.

A tanúsítvány „Country” és „Locality” mezőjében az Aláíró lakóhelyének országkódja és helységneve, a „Common Name” mezőben az Aláíró neve vagy álneve, az „E” mezőben az Aláíró e-mail címe szerepel. Amennyiben az Aláíró hozzájárul, a tanúsítvány „STREET” mezőjében az Aláíró lakcímében szereplő utca neve és a házszáma, a „PostalCode” mezőjében az Aláíró lakcímében szereplő irányítószám is szerepel. A tanúsítvány „Organization” és „Organization Unit” mezői üresen maradnak.

Az álnév jelzésére a tanúsítvány CN mezőjében található szöveg ’~’ (tilde) karakterrel kezdődik és végződik (pl. CN= „~Superman~”). Amennyiben a tanúsítvány CN mezőjében nem az aláíró azonosítására használt okmány(ok)ban szereplő név kerül megadásra, úgy ez a mező álnévként kerül rögzítésre.

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

1.5.3.2.„Szervezeti személy” („Munkatársi”) tanúsítvány

„Szervezeti személy” vagy más néven „Munkatársi” tanúsítványokat természetes személy igényelhet egy adott szervezet alkalmazottjaként és/vagy tisztségviselőjeként.

Ebben az esetben az Előfizető a szervezet, az Aláíró a szervezetet képviselő személy. Az Előfizetői Szerződésben a szervezet által vállalt kötelezettségek egyetemlegesen érvényesek a szervzetet képviselő Aláíróra.

A tanúsítvány „Country” és „Locality” mezőjében az előfizető szervezet székhelyének vagy telephelyének országkódja és városa; az „Organization” mezőben az előfizető szervezet neve; az „Organizational Unit” mezőben az igényt támasztó szervezeti egység neve (ha van ilyen); a „Common Name” mezőjen az aláírásra kijelölt szervezeti személy neve vagy álneve; a „STREET” mezőben az előfizető szervezet székhelyének vagy telephelyének címében szereplő utcanév és a házszám; a „PostalCode” mezőben a címben szereplő irányítószám; a „Title” mezőben az aláírásra kijelölt szervezeti személy beosztása (opcionálisan); az „E” mezőben az aláírásra kijelölt szervezeti személy e-mail címe szerepel.

Az álnév jelzésére a tanúsítvány CN mezőjében található szöveg ’~’ (tilde) karakterrel kezdődik és végződik (pl. CN= „~Superman~”). Amennyiben a tanúsítvány CN mezőjében nem az aláíró azonosítására használt okmány(ok)ban szereplő név kerül megadásra, úgy ez a mező álnévként kerül rögzítésre.

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

2.Általános rendelkezések

2.1. Feladatok és hatáskörök

2.1.1.A Szolgáltató feladatai és hatásköre

1. A Szolgáltató gondoskodik a szolgáltatásra vonatkozó valamennyi, a jelen HSZSZ-M-ben részletezett állítás teljesüléséről, amennyiben azok az adott tanúsítványtípusra alkalmazhatók.
2. A Szolgáltató szolgáltatásait nyilvánosan elérhetővé teszi.
3. A Szolgáltató jogi személy.
4. A Szolgáltató rendszeresen felülvizsgálja és újra kiadja HSZSZ-M-ét.
5. A Szolgáltató mindenkor az Előfizető által átadott és az Ügyfélkapcsolati Irodák által ellenőrzött adatok alapján bocsátja ki a tanúsítványokat. A Szolgáltató a tanúsítvány kibocsátását követően a tanúsítvány adataiban nem változtathat.
6. A Szolgáltató a Tanúsítványtárában teszi közzé az általa kibocsátott, a Tanúsítványok Visszavonási Listájában a felfüggesztett és visszavont előfizetői tanúsítványokat. A Tanúsítványtár, a Tanúsítványok Visszavonási Listája és az időbélyegzés szolgáltatás elérhetőségét a Szolgáltató 99,9%-os rendelkezésre állással biztosítja úgy, hogy az elérhetőség kiesése esetenként nem lépheti túl a 3 órás időtartamot.
7. A Szolgáltató kötelezettséget vállal arra, hogy a regisztrációt követő napokban, de legkésőbb 30 munkanapon belül a tanúsítvány kiadására intézkedik és erről az Előfizetőt értesíti.
8. A Szolgáltató a szolgáltatások működtetése és menedzselése során az ügyfélkapcsolati tevékenységet Ügyfélkapcsolati Irodák által biztosítja.
9. A Szolgáltató rendkívüli üzemeltetési helyzetben is biztosítja tanúsítványtára és visszavonási nyilvántartásai elérhetőségét, visszavonás kezelési, visszavonási állapot közzétételi és időbélyegzés szolgáltatását minden érdekelt fél számára. Ügyfélszolgálata útján folyamatos felügyeletet biztosít a tanúsítvány visszavonási és felfüggesztési igények fogadására és kezelésére.
10. A Szolgáltató vezeti és az Internetes honlapján keresztül bárki számára folyamatosan elérhetővé teszi a jogszabály szerinti nyilvántartásokat és a tanúsítvány kibocsátására vonatkozó saját szabályzatait.
11. A Szolgáltató a lejárat előtti 30 napban értesítést küldhet a lejáró tanúsítványokról az Előfizető részére.
12. Szolgáltató a tanúsítványban feltünteti az Előfizetői Szerződésben rögzített, a tanúsítvány felhasználhatóságával kapcsolatos korlátozásokat.
13. A Szolgáltató felfüggeszti vagy visszavonja a tanúsítványt és ezt közzéteszi ha a 4.11.1 fejezetben részletezett körülmények ezt indokolják.
14. Szolgáltató megőrzi a tanúsítványokkal kapcsolatos adatokat és az ahhoz kapcsolódó személyes adatokat legalább a tanúsítvány érvényességének lejáratától számított 10 évig, illetőleg – amennyiben ezen időszakban az elektronikus aláírással vagy az azzal aláírt elektronikus dokumentummal kapcsolatosan jogvita merül fel és azt a Szolgáltatónak írásban bejelentették – a jogvita jogerős lezárásáig. Ugyanezen határidőig olyan eszközt is biztosít, mellyel a kibocsátott tanúsítvány tartalma megállapítható.
15. Ha a Szolgáltató be kívánja fejezni tevékenységét, erről legalább hatvan nappal korábban értesíti az Előfizetőket és a Nemzeti Hírközlési Hatóságot. A bejelentés időpontjától kezdve a Szolgáltató nem bocsáthat ki új tanúsítványt. A Szolgáltató a tevékenység befejezése előtt legalább húsz nappal visszavonja az általa kibocsátott és még érvényes tanúsítványokat. A Szolgáltató a tevékenysége befejezéséig a nyilvánosságra hozatali kötelezettségének eleget tesz.
16. A Szolgáltató intézkedik az iránt, hogy legkésőbb a tevékenysége 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.

2.1.1.1.A hitelesítő központok („CA”-k) feladata

A Szolgáltató által működtetett hitelesítő központok feladata a tanúsítványok előállítása és az időbélyegzés, valamint a visszavonási listák aláírásával közreműködés a visszavonási állapot közzétételében.

A tanúsítványok előállítása során aláírják a tanúsítvány adatokat és gondoskodnak arról, hogy a kibocsátott tanúsítványokhoz tartozó kulcsok és a tanúsítványokba foglalt nevek egyediek legyenek a szolgáltatás körén belül.

A visszavonási állapot közzétételében való közreműködés keretén belül fogadják a visszavonási kérelmeket, új tanúsítvány visszavonási listát készítenek és azt aláírással hitelesítik., majd elküldik a Regisztrációs Irodátnak az aláírt tanúsítvány visszavonási listát.

Az 1. szintű „Root CA” alapvető feladata és hatásköre a 2. szintű „Produktív CA” és az időbélyegző egység hitelesítése, ezen belül a feladatok tételesen a következők:

1. Saját (szolgáltatói) kulcspár generálása és tanúsítvány előállítása önhitelesítéssel, magánkulcsának fokozott biztonságú védelme.
2. További szolgáltatói kulcspárok és tanúsítványok előállítása.
3. A 2. szintű hitelesítő központok ("Produktív CA”-k) hitelesítési kérelmeinek fogadása és ellenőrzése, részükre tanúsítványok előállítása, hitelesítése.
4. Tanúsítvány előállítása és hitelesítése az időbélyegző egység részére.
5. A „Pruduktív CA” tanúsítvány visszavonási és tanúsítvány megújítási kérelmeinek feldolgozása.
6. A „Pruduktív CA” tanúsítványainak és visszavonási listáinak publikálása a Tanúsítványtárban.

A 2. szintű „Produktív CA” Hitelesítő Központ alapvető feladata és hatásköre a Regisztrációs Iroda ("RA") és az általa regisztrált Előfizetők tanúsítványainak hitelesítése:

1. Saját szolgáltatói kulcspár generálása és magánkulcsának fokozott biztonságú védelme.
2. A Regisztrációs Iroda hitelesítési kérelmeinek fogadása és ellenőrzése.
3. Szolgáltatói kulcspár generálás és tanúsítvány előállítás a Regisztrációs Iroda részére, azok eljuttatása a Regisztrációs Irodához.
4. Előfizetői hitelesítési kérelmek fogadása a Regisztrációs Irodától és azok ellenőrzése.
5. Előfizetői kulcspár generálás és tanúsítvány előállítás, előfizetői tanúsítványok és tanúsítvány visszavonási listák publikálása a Tanúsítványtárban.
6. Regisztrációs Irodától érkező tanúsítvány visszavonási, felfüggesztési, újraérvényesítési és tanúsítvány megújítási kérelmek feldolgozása.

2.1.1.2.A Regisztrációs Iroda (RA) feladatai és hatásköre

A Regisztrációs Iroda fő feladata a hitelesítés-szolgáltatás (regisztráció, felfüggesztés és visszavonás kezelés) és az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése. Egyúttal közreműködik az előfizetői tanúsítvány előállítás, kibocsátás és visszavonási állapot közzététele szolgáltatásokban.

1. A tanúsítvány kibocsátásához szükséges ellenőrzések sikeres lefolytatása után a tanúsítvány kibocsátás elindítása a Hitelesítő Központnál, (visszautasítja a tanúsítvány kiadását, amennyiben a tanúsítvány-igénylés nem felel meg az elvárt feltételeknek).
2. Fogadja a Hitelesítő Központtól kapott előfizetői tanúsítványokat és ellenőrzi azok hitelességét és sértetlenségét.
3. Kezdeményezi a tanúsítványok elküldését a Tanúsítványtárba.
4. Előkészíti a biztonságos aláírás-létrehozó eszközt az aláírás-létrehozó eszközön történő kulcspár generáláshoz.
5. Megszemélyesíti az aláírás-létrehozó eszközt és azt személyesen eljuttatja az Ügyfélkapcsolati Irodához.
6. Előállítja a kezdeti aktivizáló adatot (PIN kódot), majd azt az aláírás-létrehozó eszköztől elkülönítve eljuttatja az Ügyfélkapcsolati Irodához.
7. Szoftveres úton történő kulcspár generálás esetén biztonságos módon eljuttatja a kulcspárt az aláírás-létrehozó eszközbe, olyan biztonságos útvonal kiépítésével, mely kriptográfiai mechanizmusok felhasználásával forráshitelesítést, sértetlenséget és bizalmasságot biztosít.
8. Biztonságos módon megsemmisíti az előállított magánkulcs aláírás-létrehozó eszközön kívüli összes példányát, miután az Aláíró részére előállított kulcspárt elhelyezte az aláírás-létrehozó eszközben.
9. Formai szempontból ellenőrzi a tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmek hitelességét és érvényességét, végrehajtja a szabályos tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket.
10. Visszautasítja a szabálytalan tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket.
11. Fogadja és feldolgozza a tanúsítvány megújítási kérelmeket.

2.1.1.3.Az időbélyegző egység feladata

1. A kérő által kezdeményezett biztonságos csatornán keresztül fogadja az időbélyegzési kérelmeket.
2. Azonosítja és hitelesíti az időbélyeg kérőt, ellenőrzi a kérelem szabályosságát.
3. Előállítja az időbélyeget, amennyiben a Szolgáltató rendszere a pontos időt biztosítani tudja.
4. A kérő által kezdeményezett biztonságos csatornán keresztül elküldi az időbélyeget a felhasználónak szabványos formában.
5. Ellenőrzi az időbélyegző szerver belső órájának pontosságát.
6. Amennyiben az óra a pontossági határon kívülre kerül, az időbélyegző szolgáltatást leállítja, és hibaüzenetet küld az Előfizetők felé.
7. Az időbélyegző szerver belső órájának az ISZR-ben előírt pontosságú szinkronizációja hiteles külső UTC idő alapján történik.

8. A belső óra pontosságának folyamatos ellenőrzése.
9. Az időbélyeg aláíró kulcs fokozott biztonságú előállítása és tárolása a 2/2002. (IV.26) MeHVM irányelvnek megfelelően.
10. Az időbélyegzéssel kapcsolatos események rögzítése, naplózása és archiválása.

2.1.1.4.Az OCSP egység feladata

1. A kérő által kezdeményezett biztonságos csatornán keresztül fogadja az OCSP kérelmeket.
2. Azonosítja és hitelesíti az OCSP állapot kérőt, ellenőrzi a kérelem szabályosságát.
3. Előállítja az OCSP választ, amennyiben a Szolgáltató rendszere a pontos időt biztosítani tudja.
4. A kérő által kezdeményezett biztonságos csatornán keresztül elküldi az OCSP választ a felhasználónak szabványos formában.
5. Ellenőrzi az OCSP szerver belső órájának pontosságát.
6. Amennyiben az óra a pontossági határon kívülre kerül, az OCSP szolgáltatást leállítja, és hibaüzenetet küld az Előfizetők felé.
7. Az OCSP szerver belső órájának az ISZR-ben előírt pontosságú szinkronizációja hiteles külső UTC idő alapján történik.
8. A belső óra pontosságának folyamatos ellenőrzése.
9. Az OCSP válasz aláíró kulcs fokozott biztonságú előállítása és tárolása a 2/2002. (IV.26) MeHVM irányelvnek megfelelően.
10. Az OCSP válaszadással kapcsolatos események rögzítése, naplózása és archiválása.

2.1.1.5.Az Ügyfélkapcsolati Iroda feladatai és hatásköre

Az Ügyfélkapcsolati Iroda szolgáltatás igénylés és teljesítés keretén belül:

1. Gondoskodik az Igénylő megfelelő tájékoztatásáról és azonosításáról.
2. Ellenőrzi a 3.1 pontban és az ÁSZF-M-ben előírt adatszolgáltatási követelmények szerint megadott adatok alapján a szolgáltatást igénylő ügyfél személyazonosságát és az Aláíró adatait.
3. Meghatározza a tanúsítványba kerülő adatokat, ellenőrzi az Igénylő által átadott dokumentumok valódiságát, érvényességét, sértetlenségét és hitelességét.
4. Lehetőség szerint ellenőrzi a dokumentumok érvényességét, valódiságát valós idejű nyilvántartásokban is
5. előkészíti az Előfizetői Szerződést.
6. Elszámolja és kiszámlázza a szolgáltatások ellenértékét.
7. Nyilvántartásba veszi a regisztráció során felvett adatokat és megőrzi azokat.
8. Bizalmas információként kezeli az Előfizető és az Aláíró minden adatát, kivéve azokat, amelyek a tanúsítványba kerülnek.
9. Gondoskodik az aláírás-létrehozó eszköz és a PIN boríték biztonságos kezeléséről és átadásáról.
10. Tájékoztatja az Előfizetőt a tanúsítványa lejáratát megelőző 30 napban.
11. Az Aláíró adatainak változása és tanúsítvány megújítási kérelem esetén ellenőrzi a már korábban nyilvántartásba vett adatokat és intézkedik a Regisztrációs Iroda felé a kérelem teljesítésére.
12. Kezeli a szolgáltatással kapcsolatos bejelentéseket, kérdéseket, panaszokat.

A visszavonás kezelés szolgáltatás keretén belül:

1. Ellenőrzi a tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmek hitelességét.
2. Visszautasítja (az ok megjelölésével) a nem hiteles vagy szabálytalan, tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket.
3. A visszavonási kérelem elfogadása után intézkedik a tanúsítvány visszavonására.
4. Tájékoztatja a visszavont, illetve felfüggesztett tanúsítvány tulajdonosát tanúsítványa állapotának változásáról.

2.1.1.6.A Hitelesítési Rend és Szabályozási Csoport feladatai és hatásköre

A Hitelesítési Rend és Szabályozási Csoport a hitelesítés-szolgáltatást nyújtó szervezeti egységtől függetlenül működik. Kötelessége a Szolgáltató és felhasználó Közösség igényeinek felmérése és folyamatos követése, ezek alapján a közösség működésére vonatkozó alapelvek, politikák lefektetése, s ebből levezetve a tagok tevékenységét részletesen szabályozó, az egész Szolgáltató szervezetre nézve közös szabályzatok, így a hitelesítési politikák, a HSZSZ-M, az ISZR, az ÁSZF-M, az Előfizetői Szerződések és a Biztonsági Szabályzat, készítése és rendszeres karbantartása változatkövetéssel.

A Hitelesítési Rend és Szabályozási Csoport feladatai tételesen a következők:

1. A hitelesítési-, és időbélyegzési szolgáltatási rendek elkészítése és karbantartása.

2. A hitelesítés-szolgáltatási szabályzatok és az általános szerződési feltételek elkészítése és karbantartása.
3. A hitelesítési rendek és szabályzatok közötti összhang biztosítása.
4. A szolgáltatói szabályzatok verzióinak nyilvántartása és megőrzése.
5. Nyilvános szabályzatok publikálása.
6. A regisztrációs folyamat szabályozása, ellenőrzése, felülvizsgálata.

2.1.1.7.Az Ügyfélszolgálat feladata

A tanúsítványokkal kapcsolatos felfüggesztési, illetve visszavonási kérelmeket a Szolgáltató Ügyfélszolgálata telefonon és elektronikus levélben folyamatosan (napi 24 órában) fogadja.

2.1.2.Az Előfizető és az Aláíró feladatai és hatásköre

Az Előfizető és az Aláíró kötelessége a Szolgáltató szerződéses feltételeinek és szabályzatainak megfelelően eljárni a szolgáltatás igénybevétele során. Ennnek során az Előfizető és az Aláíró köteles:

1. Önmagát az Ügyfélkapcsolati Irodán hiteles okmányokkal igazolni.
2. A tanúsítvány igénylését és magánkulcsának felhasználását úgy végezni, hogy az harmadik fél jogait ne sértse.
3. Az Előfizető a regiszrtráció során atanúsítvány kiadásához szükséges adatokat ellenőrizni.
4. Az Aláíró biztosítani az aláírás-létrehozó eszközének és adatának, valamint a PIN kódjának védelmét.
5. Az Előfizető, illetve az Aláíró 3 (három) munkanapon belül jelezni Szolgáltatnál a regisztráció során felvett adataiban történő változásokat, különös tekintettel a tanúsítványba foglalt adatokra.
6. Az Aláíró az aláírás-létrehozó adatát csak az előfizetői szerződésben rögzített korlátozásoknak megfelelően használhatja.
7. Az Aláíró tudomásul venni, hogy magánkulcsának védelme és az elektronikus aláírás készítése kizárólag a saját felelőssége, ezért ezzel - így különösen a magánkulcsának illetéktelen harmadik személyhez kerülésével - kapcsolatban a Szolgáltatót semmiféle felelősség nem terheli.
8. Az Előfizető az ÁSZF-M módosításáról szóló értesítést követően 72 órán belül az Aláírókat írásban tájékoztatni a változásokról.
9. Az Aláíró azonnal intézkedni tanúsítványának visszavonása, illetve felfüggesztése végett, ha az aláírás létrehozó adat és/vagy a PIN kód nem az Aláíró kizárólagos birtokában van (elveszett, ellopták, esetleg kompromittálták), vagy ennek alapos gyanúja áll fenn.
10. Kompromittálódás esetén az Aláíró magánkulcsának használatát azonnal és véglegesen megszakítani,
11. az Aláíró vagy az Előfizető a Tanúsítvánnyal ellátott elektronikus dokumentummal kapcsolatos jogvita megindulásáról köteles haladéktalanul tájékoztatni a Szolgáltatót.
12. Az időbélyeget felhasználók kötelesek a kért időbélyeg vétele után meggyőződni arról, hogy az időbélyeget a Szolgáltató elektronikusan aláírta, az aláírás az időbélyegzésre szolgáló kulccsal történt-e és a hozzátartozó tanúsítvány érvényes-e.
13. Az OCSP válasz felhasználók kötelesek a kért OCSP válaszok vétele után meggyőződni arról, hogy azt a Szolgáltató elektronikusan aláírta, az aláírás az OCSP válaszadásra szolgáló kulccsal történt-e és a hozzátartozó tanúsítvány érvényes-e.

Továbbá:

1. Az Aláíró jogosult arra, hogy a magánkulcsot birtokolja és a jogszabályokban meghatározott módon elektronikus aláíráshoz felhasználja.
2. Az Aláíró tudomásul veszi, hogy a magánkulcsával készített elektronikus aláírás a saját elektronikus aláírásának minősül, és viseli ennek jogkövetkezményeit.

2.1.3.Érintett félre vonatkozó ajánlások

Az Érintett félnek ajánlott (a Szolgáltató szabályzataiban leírtaknak megfelelően) a legnagyobb gondossággal eljárni az Elektronikus aláírás és a tanúsítvány elbírálásakor, ezen belül:

1. Az Elektronikus aláírás elfogadása előtt indokolt megértenie az Elektronikus aláírással kapcsolatos technikai, jogi, biztonsági és egyéb vonatkozásokat.
2. Ajánlott megismernie Szolgáltató nyilvánosan elérhető szabályzatait (HSZSZ-M, ÁSZF-M).
3. Elfogadás előtt indokolt elvégeznie az elektronikus aláírás ellenőrzését az Aláíró tanúsítványának segítségével, meggyőződve az üzenet eredetiségéről és az aláírás valódiságáról.
4. A tanúsítványban feltűntetett azonosító alapján, a rendelkezésre álló egyéb adatok és törvényes módszerek segítségével indokolt egyértelműen meggyőződnie az Aláíró személyéről.
5. Indokolt ellenőriznie a tanúsítvány érvényességét és hatályosságát a tanúsítványban megadott adatok alapján.

6. Különösen indokolt elvégeznie a teljes tanúsítási lánc ellenőrzését az alábbiak szerint:
   6.1 Meggyőződnie a tanúsítvány kibocsátójának kilétéről a kibocsátó (Szolgáltató) azonosítója alapján..
   6.2 Meggyőződnie az Aláíró tanúsítványának integritásáról a Szolgáltató tanúsítványának segítségével.
   6.3 Ajánlott ellenőriznie a tanúsítvány állapotát a tanúsítvány visszavonási listák (CRL) áttanulmányozásával vagy OCSP szolgáltatás igénybe vételével.
   6.4 Ajánlott tanulmányoznia a tanúsítvány összes attribútumát, és az adott tranzakcióra vonatkozó előírásoknak, valamint józan megfontolásoknak megfelelően döntést hozni az aláírás elfogadásáról.
7. Az Elektronikus aláírás elfogadását vissza kell utasítani, ha az Elektronikus aláírás, az Aláíró tanúsítványa, vagy a tanúsítási lánc tanúsítványainak valamely adata, annak érvénytelenségére utal, illetve ha az az adott kontextusban nem elfogadható; az aláírás elfogadása nem jelenti az aláírt üzenet tartalmának tudomásul vételét vagy elfogadását.
8. Az időbélyeget aláíró kulcs tanúsítványának az Érintett fél által történő ellenőrzésére vonatkozóan általában érvényesek a 2.2.3 pontban leírt, a tanúsítvány ellenőrzésre vonatkozó szabályok.
9. Egy időbélyeggel ellátott állomány átvétele után az Érintett félnek indokolt ellenőriznie a Szolgáltató általi aláírás megtörténtét, a Szolgáltató időbélyeget aláíró kulcsához tartozó tanúsítvány érvényességét a Visszavont Tanúsítványok Listája segítségével a 2.1.2 pontban leírt módon.
10. Az OCSP választ aláíró kulcs tanúsítványának az Érintett fél által történő ellenőrzésére vonatkozóan általában érvényesek a 2.2.3 pontban leírt, a tanúsítvány ellenőrzésre vonatkozó szabályok.
11. Egy OCSP válasszal ellátott állomány átvétele után az Érintett félnek indokolt ellenőriznie a Szolgáltató általi aláírás megtörténtét, az Szolgáltató OCSP választ aláíró kulcsához tartozó tanúsítvány érvényességét a Visszavont Tanúsítványok Listája segítségével a 2.1.2 pontban leírt módon.
12. Az ellenőrzés a tanúsítvány érvényességének lejárta után is elvégezhető, mert a Szolgáltató az Eat. 9.§ (7. bek.) alapján a tanúsítványokat és a tanúsítványok ellenőrzéséhez szükséges adatokat a tanúsítvány lejártát követő 10 évig, illetve az aláírt és/vagy időbélyegzett és/vagy OCSP válaszzal elátott dokumentummal kapcsolatban felmerült jogvita lezárásáig megőrzi, így a tanúsítványokkal kapcsolatos elektronikus információkat és ahhoz kapcsolódó személyes adatokat elő lehet keresni és a tanúsítvány érvényességét ellenőrizni lehet. A tanúsítvány tartalmának megállapításához a Szolgáltató megfelelő eszközt biztosít.

2.2. Felelősségek

2.2.1. A Szolgáltató felelőssége

A Szolgáltató azzal, hogy aláír egy, a jelen HSZSZ-M 1.5 pontja szerint meghatározott tanúsítványt, időbélyeget, illetve OCSP választ – és ezzel jelzi az 1.4 pontban meghatározott felhasználó közösség felé ezen HSZSZ-M használatát – azért vállalja a felelősséget, hogy a tanúsítvány előállítása, kibocsátása, közzététele, visszavonása, a Visszavonási Lista közzététele, az időbélyegzés és OCSP válaszadás tevékenységek a jelen HSZSZ-M-ben előírtaknak teljes mértékben megfelelnek, és a Szolgáltató megteszi a szükséges intézkedéseket ahhoz, hogy a Szolgáltató maga és az Előfizetők is a jelen HSZSZ-M előírásainak megfelelően járjanak el.

A Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személlyel szemben a Magyar Köztársaság Polgári Törvénykönyvéről szóló 1959. évi IV. törvény 339. §-a szerint felelős az elektronikus aláírással aláírt elektronikus dokumentummal okozott kárért, ha mulasztása bizonyítható.

A Szolgáltató a vele szerződéses jogviszonyban álló Előfizetővel szemben a szerződésszegésért való felelősség szabályai szerint felelős az elektronikus aláírással aláírt elektronikus dokumentummal okozott kárért, ha megszegte a HSZSZ-M-ben, az ÁSZF-M-ben vagy az előfizetői szerződésben előírtakat, továbbá az Eat. 7. § (2) bekezdésében, a 9-11. §-okban vagy a 14.§-ban foglaltakat. E szabályok megtartását kétség esetén a szolgáltatónak kell bizonyítania.

A felelősségvállalás mértékét, mely tanúsítvány típusonként és egyedi tanúsítványonként is maximált összegű, az Előfizetői Szerződésben kell rögzíteni.

A Szolgáltató nem vállal felelősséget, ha a Szolgáltató által kibocsátott tanúsítvány a jelen HSZSZ-M-ben előírtaktól eltérő módon kerül felhasználásra. Így a Szolgáltató nem felelős az olyan károkért, melyek abból adódtak, hogy az Érintett fél a tanúsítványok ellenőrzése és felhasználása során nem a hatályos jogszabályok és Szolgáltató HSZSZ-M-e szerint járt el, illetve nem tanúsította a tőle elvárható gondosságot.

A Szolgáltató azáltal, hogy az Előfizetők részére tanúsítványokat, időbélyegeket vagy OCSP válaszokat bocsát ki, semmilyen körülmények között sem tekinthető az Előfizetők vagy az érintett felek ügynökének, megbízottjának, képviselőjének, vagy bármilyen más, az Előfizetői Szerződésben meghatározottól eltérő funkciójú partnerének a hitelesítési tevékenysége vonatkozásában.

2.2.2. Az Előfizető és az Aláíró felelőssége

Az Előfizetőnek és az Aláírónak felelőssége áll fenn a regisztráció során megadott adatainak valódiságával kapcsolatban.

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

Az Előfizető vagy az Aláíró köteles azonnal tájékoztatni a hitelesítés-szolgáltatót az aláírás-létrehozó adatnak illetéktelen személy tudomására jutásáról vagy elvesztéséről.

Az Előfizető vagy az Aláíró köteles három napon belül tájékoztatni a hitelesítés-szolgáltatót, ha:

a. az azonosításához szükséges személyazonosító adatokról, más személy (szervezet) képviseletében történő aláírásra jogosító elektronikus aláírás esetén a képviseletre, illetőleg aláírásra jogosult személy személyazonosító adatairól, a cégadatokról, továbbá mindezek változásáról;

b. az aláírással vagy az így aláírt elektronikusan aláírt elektronikus dokumentummal, illetve a tanúsítvánnyal kapcsolatban észlelt - a szolgáltatási szabályzatban meghatározott - rendellenességről;

c. a tanúsítvánnyal ellátott elektronikusan aláírt elektronikus dokumentummal, időbélyeggel vagy OCSP válasszal kapcsolatos jogvita megindulásáról.

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

Az időbélyeget kérő fél felelős az időbélyeg aláírás helyességének és az időbélyeg aláíró kulcs tanúsítványa érvényességének az időbélyegzett állomány vételekor elvégzendő, a 2.1.2 pont szerinti ellenőrzésért.

Az OCSP választ kérő fél felelős az OCSP válasz aláírás helyességének és az OCSP választ aláíró kulcs tanúsítványa érvényességének az OCSP választ tartalmazó állomány vételekor elvégzendő, a 2.1.2 pont szerinti ellenőrzésért.

A Szolgáltató nem vállal felelősséget a biztonságos aláírás-létrehozó eszköz hordozó elvesztéséből, vagy az aláírás-létrehozó adat (magánkulcs) biztonságának egyéb módon történő sérüléséből, elvesztéséből, illetve a PIN kód illetéktelen személy tudomására jutásából származó károkért.

2.2.3. Érintett fél felelőssége

Az Érintett fél felelős az elektronikus aláírás és a Szolgáltató által kibocsátott tanúsítványok elfogadása során tanúsított körültekintő ellenőrzésért, valamint a Szolgáltató nyilvánosan elérhető HSZSZ-M-je rá vonatkozó részének megismerésért.

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

2.3. Az anyagi felelősség mértéke

A Szolgáltató anyagi felelősségének mértékéről, illetve annak korlátairól az ÁSZF-M rendelkezik.

A Szolgáltató az anyagi 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 azokat (lásd: 4.12.1 és 4.13 fejezetek).

2.4. Értelmezés és alkalmazás

2.4.1. Irányadó jog

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

A Szolgáltató tevékenységére elsősorban a következő jogszabályok mérvadók:

2001. évi XXXV. törvény (Eat.),

2/2002. (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről,

3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

9/2005. (VII. 21.) IHM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról,

45/2005. (III. 11.) Korm. rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól

20/2001. (XI.15.) MeHVM rendelet a Hírközlési Felügyeletnek az elektronikus aláírással összefüggő nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról,

7/2002 (IV.26) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről.

Ezeken túlmenően a Szolgáltató az üzleti titkok vonatkozásában az 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról, a személyes adatok vonatkozásban az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról és az 1995. évi CXXII. törvény a polgárok személyes adatainak nyilvántartásáról szóló 1992. évi LXVI. tv. módosításáról szerint jár el.

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

2.4.2. Érvénytelenség, hatályosság, megszűnés, értesítések

2.4.2.1. Érvénytelenség

Ha a Szolgáltató szerződéseinek vagy szabályzatainak valamely pontja érvénytelenné vagy érvényesíthetetlenné válik, az a szabályzat vagy szerződés egyéb pontjainak érvényességét nem érinti.

A jelen HSZSZ-M minden olyan rendelkezése, amelyek a felelősségek, a kötelezettségek, garanciák és a kártérítés korlátaira vonatkoznak, azok függetlenül más intézkedésektől, önmagukban értelmezendők és érvényesítendők.

2.4.2.2. Hatályosság

A HSZSZ-M és az ÁSZF-M a felhasználói közösség résztvevőinek valamennyi kötelezettségét, felelősségét és jogát tartalmazza. A HSZSZ-M egyetlen pontja sem értelmezhető a jelen dokumentumba foglalt értelmezéstől eltérően. A HSZSZ-M csak írott és hitelesített formában módosítható, a Nemzeti Hírközlési Hatóság által vezetett nyilvántartásban való átvezetés mellett.

A HSZSZ-M időbeli hatálya a Szolgáltató Nemzeti Hírközlési Hatóság általi nyilvántartásba vételének keltétől a szolgáltatási tevékenység megszűntéig tart. A HSZSZ-M személyi és tárgyi hatályát az 1.4.4.1 pont tartalmazza.

2.4.2.3. Megszűnés

A HSZSZ-M a Szolgáltató működésének befejezésével tekintendő megszűntnek.

2.4.2.4. Értesítések

Az Előfizetők, az Aláírók és az Érintett felek vagy bármely harmadik fél az Ügyfélkapcsolati Irodát munkanapokon megkeresheti ügyfélfogadási időben személyesen vagy telefonon, postai úton írásban, e-mail-ben vagy faxon. A Szolgáltató Ügyfélszolgálata (Help Desk) folyamatos (7x24 órás) szolgálattal áll rendelkezésre telefonos vagy e-mail megkeresés esetén. Az írásban vagy elektronikus úton történő kommunikáció esetében a feladó nevét és elérhetőségét fel kell tüntetni és a feladónak a küldeményt hitelesítenie kell.

A Szolgáltató az Előfizetőket és Érintett feleket tipikusan az Internetes honlapján (web oldalain) történő közzététellel, illetve az ügyfélkapcsolati irodákban elérhető dokumentumokkal tájékoztatja. Az ügyfélkapcsolati irodák az Előfizetőket esetenként írásban vagy elektronikus úton is értesíthetik.

2.4.3. Vitás kérdések kezelése

Bármely vitás kérdés felmerülése esetén az Előfizetőnek kötelessége a Szolgáltató haladéktalan értesítése és teljeskörű tájékoztatása a kérdés minden vonatkozását érintően, a vita jogi útra terelése előtt.

Panaszt az Előfizetőt nyilvántartó Ügyfélkapcsolati Irodán vagy az Ügyfélszolgálatnál lehet írásban vagy szóban előterjeszteni. A panaszt a Szolgáltató az előterjesztéstől számított 20 munkanapon belül kivizsgálja és ennek eredményéről a panaszost írásban tájékoztatja.

A jogviták esetén követendő eljárást az ÁSZF-M tartalmazza.

2.5. Díjak

A mindenkor érvényes szolgáltatási díjakat a Szolgáltató Internetes honlapján keresztül teszi közzé. A Szolgáltató jogosult az árlistát egyoldalúan módosítani.

Az Előfizetőkre vonatkozó hatályos szolgáltatási díjak az Előfizetői Szerződésben kerülnek rögzítésre.

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

2.5.1. Tanúsítvány kibocsátás

Szolgáltató a kibocsátott és megújított tanúsítványokért éves fenntartási díjat számol fel az Előfizető felé, amely tartalmazza a tanúsítványok kibocsátásának (illetve megújítás esetén megújításának) és Tanúsítványtárban történő közzétételének díját az érvényesség időtartamára, valamint a tanúsítványok lejárat utáni archiválásának a díját.

2.5.2. Tanúsítvány hozzáférés

Szolgáltató a közzétett tanúsítványok eléréséért nem számol fel díjat.

2.5.3. Visszavonási lista hozzáférés

A Szolgáltató a közzétett visszavonási lista eléréséért nem számol fel díjat.

2.5.4. Időbélyegzés

A Szolgáltató az időbélyegek kibocsátásáért az erre vonatkozó szerződés keretében meghatározott díjat számol fel.

2.5.5. OCSP szolgáltatás

A Szolgáltató az OCSP szolgáltatásért az Előfizetői Szerződésben meghatározott díjat számol fel.

2.5.6. Egyéb szolgáltatásokra vonatkozó díjak

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

2.5.7. Visszatérítési elvek

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

- *a.* a kibocsátott tanúsítvány valamely adata a Szolgáltató hibájából fakadóan nem megfelelő,
- *b.* a kibocsátott tanúsítvány, magánkulcs és aktivizáló adat nem összetartozó,
- *c.* a kibocsátott aláírás-létrehozó eszközön szereplő adatok a Szolgáltató hibájából fakadóan nem megfelelők,
- *d.* a kibocsátott aláírás-létrehozó eszköz, az aktivizáló kód és a kulcsok nem összetartozók,
- *e.* a Szolgáltató bizonyítottan nem tartja be valamely kötelezettségét Előfizető tanúsítványának kezelésekor.

A díj visszatérítésére vonatkozó igényt Előfizetőnek a tanúsítvány kibocsátását, illetve megújítását követő 30 naptári napon belül a regisztrációt végző ügyfélkapcsolati irodánál kell beadnia Szolgáltató részére. A kérvény pozitív elbírálása esetén a Szolgáltató a tanúsítványt díjmentesen visszavonja és a fenntartási díjat az Előfizető számára a megjelölt bankszámlaszámra 20 naptári napon belül visszautalja, vagy részére új tanúsítványt bocsát ki.

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

A Szolgáltató egyéb tevékenységeiért számlázott díjak esetében díjvisszafizetésre nem köteles.

2.6. Közzététel

2.6.1. Tanúsítványtár

A Szolgáltató az általa kibocsátott tanúsítványokat és a tanúsítvány visszavonási listákat tanúsítványtárában helyezi el.

Az Aláíró vagy az Érintett fél a szolgáltatás internetes honlapján keresztül érheti el a Tanúsítványtár adatait.

A Tanúsítványtár elérhetőségét a Szolgáltató folyamatosan (az év minden napján, 24 órában), 99,9%-os rendelkezésre állással biztosítja úgy, hogy a Tanúsítványtár szolgáltatás kiesése nem lépheti túl esetenként a 3 órás időtartamot.

2.6.2. A tanúsítványokra vonatkozó információk közzététele

A Szolgáltató gondoskodik arról, hogy az általa kibocsátott tanúsítványok[5], a tanúsítványok használatának feltételei és egyéb közérdekű szolgáltatói információk az Előfizetők és az érintett felek részére folyamatosan rendelkezésére álljanak:

a. tanúsítvány típusok
b. tanúsítványok használatára vonatkozó ismertetők, szabályzatok, nyomtatványok
c. kibocsátott előfizetői és szolgáltatói tanúsítványok
d. felfüggesztett és visszavont előfizetői és szolgáltatói tanúsítványok
e. szolgáltatói közlemények

A Szolgáltató a szolgáltatói információkat elektronikus formában Internetes honlapján keresztül teszi elérhetővé. Szolgáltatónak csak saját elektronikus aláírásával ellátott dokumentumai tekinthetők eredetinek. Az elektronikus dokumentumok nyomtatott változatai nem tekinthetők hivatalos példánynak vagy hiteles másolatnak.

A Szolgáltató hiteles nyomtatott dokumentumai az Ügyfélkapcsolati Irodán férhetők hozzá.

2.6.3. A közzététel gyakorisága

Tanúsítványok, kikötések és feltételek nyilvánosságra hozatala:

A Szolgáltató a kibocsátott előfizetői tanúsítványokat - az érintett alany, illetve előfizető hozzájárulása esetén - a Tanúsítványtárban 24 órán belül közzéteszi és azok elérhetőségét az Interneten keresztül korlátozás nélkül, folyamatosan, a 2.6.1 pont szerinti rendelkezésre állással biztosítja.

A Szolgáltató általa működtetett hitelesítő központok szolgáltatói tanúsítványait a Tanúsítványtárában 24 órán belül közzéteszi és azok elérhetőségét az Interneten keresztül korlátozás nélkül, folyamatosan, a 2.6.1 pont szerinti rendelkezésre állással biztosítja..

A Szolgáltató a HSZSZ-M-ben és az ÁSZF-M-ben tervezett változásokról a hatályba lépést megelőzően legalább 30 nappal tájékoztatja a Nemzeti Hírközlési Hatóságot. A változások hatályba léptetéséhez a hatóság hozzájárulása szükséges.

Visszavonási állapot információk nyilvánosságra hozatala:

a.) A Szolgáltatónak a visszavonási és felfüggesztési kérelem fogadásától számított 3 órán belül meg kell állapítania a kérelem érvényességét (a kérelmező jogosultságát), és a Visszavont Tanúsítványok Listájában át kell vezetnie az érvényes kérelem szerinti visszavonási állapot megváltozását.

b.) A Szolgáltató a kérelem szerint módosított visszavonási állapotot az *a.)* pontban foglaltak teljesítését követő 1 órán belül teszi közzé a Visszavont Tanúsítványok Listájában.

c.) A Szolgáltató a tanúsítvány visszavonási listákat (beleértve ezek bármely változatát is) legalább 24 óránként teszi közzé.

A Szolgáltató a Visszavont Tanúsítványok Listájának elérhetőségét az Interneten keresztül korlátozás nélkül, folyamatosan, a 2.6.1 pont szerinti rendelkezésre állással biztosítja.

2.6.4. Elérési szabályok

A Szolgáltató minden Előfizető és Érintett fél számára elérhetővé teszi a szolgáltatás Internetes honlapját, ezen keresztül Tanúsítványtárát olvasás céljából. A Tanúsítványtárban keresési lehetőséget biztosít a tanúsítvány sorszáma és azonosító adatai alapján.

A Szolgáltató belső adatbázisait és egyéb adatállományait csak és kizárólag a Szolgáltató biztonsági szabályzatai által meghatározott szerepkörű és jogosultságú munkatársai érhetik el egyénileg differenciált azonosítás-hitelesítési és feljogosítási eljárásban.

2.7. A megfelelőség vizsgálata

A Szolgáltatót a Nemzeti Hírközlési Hatóság jogelődje, a Hírközlési Felügyelet minősített hitelesítés-szolgáltatóként 2003. április 3.-án nyilvántartásba vette.

A Nemzeti Hírközlési Hatóság a Szolgáltató bejelentése alapján a jelen dokumentumban megnevezett biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített tanúsítványt nyilvántartásába felvette.

A Szolgáltató minősített hitelesítés-szolgáltatásához olyan biztonságos elektronikus aláírási termékeket használ, amelyek szerepelnek a Nemzeti Hírközlési Hatóság „tanúsított elektronikus aláírási termékek” listáján.

A Szolgáltató az időbélyegzés szolgáltatásához olyan biztonságos aláírás létrehozó eszközt használ, mely szerepel a Nemzeti Hírközlési Hatóság „tanúsított elektronikus aláírási termékek” listáján.

[5] Az előfizetői tanúsítványokat a Szolgáltató csak az Előfizető hozzájárulásával teszi közzé

A Szolgáltató a hitelesítés-szolgáltatási, OCSP szolgáltatási és időbélyegzési tevékenységét, a szolgáltatást támogató informatikai rendszert, valamint annak személyi és fizikai környezetének biztonságát auditáltatja, illetve tanúsíttatja:

a. a saját szervezetén belüli belső auditor szervezettel

b. független külső auditor céggel

A Szolgáltató a szolgáltatási rendszerének következő elemeit auditáltatja:

a. Az előfizetői és szolgáltatói minősített tanúsítványok kezeléshez és az időbélyegzéshez felhasznált elektronikus aláírási termékeit

b. Az előfizetői és szolgáltatói minősített tanúsítványok kezeléshez, az időbélyegzéshez és az OCSP szolgáltatáshoz használt rendszereit és módszereit

A Szolgáltató a magánkulcsainak tárolására használt az aláírás-létrehozó eszközeit tanúsíttatja. A tanúsításhoz a Szolgáltató külső szervezetet vesz igénybe.

A Szolgáltató az Eat. 8/b § szerint önkéntes akkreditációs rendszer keretében nem lett tanúsítva.

2.7.1. Vizsgálatok gyakorisága

A Szolgáltató aláírás-létrehozó eszközözének tanúsítására a használatba vételt megelőzően egyszer került sor.

A Szolgáltató az Előfizetők számára tanúsított biztonságos aláírás-létrehozó eszközöket (BALE) biztosít.

A Nemzeti Hírközlési Hatóság a jogszabályoknak megfelelően évente átfogó helyszíni ellenőrzést végez.

A Szolgáltató a külső, illetve a saját ellenőrző szervezete által végzett belső vizsgálatokat a Biztonsági Szabályzatában megjelölt rendszerességgel végezteti, illetve végzi.

2.7.2. Az átvizsgáló szervezet megnevezése/jellemzői

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

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

2.7.3. Hiányosságok kezelése

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

2.7.4. Eredmény kommunikációja

A hiányosságok felszámolásáról a Szolgáltató Nemzeti Hírközlési Hatóságot tájékoztatja.

A Szolgáltató nem köteles a feltárt konkrét hiányosságokat nyilvánosságra hozni.

2.8. Bizalmasság – Adatkezelési szabályok

2.8.1. Bizalmas információk

Szolgáltató az előfizetői adatokat csakis és kizárólag a hitelesítési-szolgáltatással összefüggésben használja fel.

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

a. A fontos bejegyzéseket védi az elveszéstől, tönkretételtől és hamisítástól

b. megfelelő technikai és szervezeti intézkedéseket hoz a személyes adatok felhatalmazás nélküli, illetve törvénysértő kezelése ellen

c. nyilvántartásba veszi az Előfizetővel aláírt szerződést, beleértve az Előfizető hozzájárulását az alábbiakhoz:

- hozzájárulás a szolgáltatások során felhasznált adatok hitelesítés-szolgáltató által történő nyilvántartásba vételéhez
- hozzájárulás a nyilvántartásba vett adatok harmadik félhez történő továbbításához, a Szolgáltató szolgáltatásainak leállítása esetén
- a tanúsítvány közzétételéhez

d. csak annyi bizonyítékot követel meg az azonosításhoz, mely elégséges a tanúsítvány tervezett felhasználásához

e. gondoskodik az Előfizetőre és az Aláíróra vonatkozó adatok bizalmas kezeléséről, kivéve, ha felfedésükhöz ők maguk[6] hozzájárulnak, vagy ha bíróság, illetve egyéb jogi követelmény ezt előírja,

f. védi a regisztrációs adatok bizalmasságát (és sértetlenségét) az Előfizetővel folytatott adatcsere során is

A bizalmasság szempontjából legmagasabb érzékenységi szintet képviselő Aláírók aláírás-létrehozó adatait és a szolgáltatói aláírás-létrehozó adatokat, illetve az ezeket hordozó eszközöket, aktiváló kódokat fokozott biztonsággal kezeli.

A Szolgáltató tevékenysége során a következő bizalmas adatköröket kezeli:

a. a Szolgáltató üzleti titkai

b. az Előfizető Társaságok által a Szolgáltatónak átadott üzleti titkok

c. az Előfizetők és az Aláírók személyes adatai

Az 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 személyes adatok vonatkozásban az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról és az 1995. évi CXXII. törvény a polgárok személyes adatainak nyilvántartásáról szóló 1992. évi LXVI. törvény módosításáról szóló törvény.

A Fentiek értelmében a Szolgáltató az Előfizetők és az Aláírók személyes adatait csak a közöttük fennálló Előfizetői Szerződéssel összhangban levő célokra használhatja fel, harmadik félnek azokat az Előfizetők és az Aláírók írásos hozzájárulása nélkül nem adhatja át, kivéve a 2.8.4 pontban meghatározott eseteket.

A Szolgáltató által kezelt adatok egy része a nyilvános kulcs tulajdonosának azonosítása céljából a tanúsítványba foglalva a Szolgáltató tanúsítványtárán keresztül – Előfizető és Szolgáltató ilyen irányú megállapodása esetén - nyilvánosságra kerül, másik részét a Szolgáltató védett módon tárolja az Előfizető és az Aláíró azonosságának igazolása és egyéb adatszolgáltatási kötelezettségei céljából.

2.8.2. Nem bizalmas információk

A Szolgáltató a regisztrációs űrlapon külön jelöli mindazon adatokat, melyek a Tanúsítványtárban hozzáférhető előfizetői tanúsítványban nyilvánosságra kerülnek.

2.8.3. Tanúsítvány visszavonási és felfüggesztési okok felfedése

A Szolgáltató az általa kibocsátott tanúsítványok felfüggesztését és visszavonását tanúsítvány-visszavonási listákban, illetve OCSP szolgáltatás keretében teszi közzé.

A Szolgáltató a tanúsítvány visszavonás okát a vonatkozó szabványok által támogatott módon feltünteti a visszavonási listában, illetve az OCSP kérésekre adott válaszaiban. Ezen kívül a visszavonással kapcsolatos minden egyéb adatot bizalmasan kezel.

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 – az Eat. 11.§ paragrafusa alapján adatokat továbbít a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak.

Az adatátadás tényét rögzíteni kell, az adatátadásról a Szolgáltató sem az Előfizetőt sem az Aláírót 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 - az Aláíró személyazonosságát igazoló adatokat átadhatja az ellenérdekű peres félnek vagy képviselőjének feltárhat bizalmas felhasználói információkat, illetőleg azt közölheti a megkereső bírósággal az Eat. 11.§ paragrafusa alapján.

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

[6] vagy nevükben az Előfizető

2.8.6. Feltárás tulajdonos kérésére

Szolgáltató a törvényi meghatalmazással rendelkezők részére történő adatszolgáltatáson túl más Társaság üzleti titkát, az Előfizetők és az Aláírók nem nyilvános személyes adatait csak az Illető Társaság illetve Előfizető írásos 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 az Eat. 16. § (2.) bek. szerint.

2.9. Szellemi tulajdonhoz fűződő jogok

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

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

A Szolgáltató tulajdonát képezik:

a. a visszavonási információk

b. a Szolgáltató által az Aláíró részére kibocsátott egyedi azonosító

c. a Szolgáltató szabályzatai, szerződéses feltételei

d. a tanúsítványban szereplő hitelesítő azonosító

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

A tanúsítványban szereplő megkülönböztető név használatára az Előfizető jogosult.

3.Azonosítás és hitelesítés

3.1. Regisztráció

A Szolgáltató a tanúsítvány igényléséhez szükséges regisztráció során:

a. gondoskodik arról, hogy az Előfizető tanúsítvány kérelmei pontosak, hitelesek és teljesek legyenek

b. megfelelő források igazolásán alapulva megvizsgálja az Aláírók és Előfizetők azonosságára vonatkozó bizonyítékokat, valamint nevük és a hozzá kapcsolódó adatok pontosságát

Ha egy Igénylő csak időbélyegzés szolgáltatást igényel, a regisztráció egyszerűsített eljárással történik a 3.1.11 pont szerint.

3.1.1. Nevek típusa

A tanúsítványokban szereplő névmegadás az ITU-T[7] X.500 ajánlásának felel meg: X.500 formátum (ITU-T X.501 /ISO/IEC 9594-2:1997, RFC 2459).

3.1.2. Nevek szemantikája

Megnevezési konvenciók:

A tanúsítványban szerepeltetendő nevek megadásakor a Szolgáltató a következő szabályok szerint jár el:

A tanúsítványban szereplő adatok magyar vagy angol írásmód szerint, a magyar ABC írásjeleit felhasználva, speciális és vezérlő karakterek nélkül kerülnek rögzítésre. A Szolgáltatót fenntartja a jogot, hogy tanúsítvány adatok egyedi elbírálás alapján az előzőektől eltérő írásmód vagy karakterkészlet használatával kerüljenek rögzítésre.

A tanúsítványokban szereplő nevek (Common Name mező adatai) általában valódi nevek, de lehetnek álnevek is. A Szolgáltató fenntartja a jogot az egyes személyeket vagy csoportokat esetlegesen sértő (pl. jóízlést, szemérmet, etnikai hovatartozást sértő) álnevek és egyéb adatok megadásának elutasítására.

A Ket. hatálya alá tartozó név típusok:

Természetes személy alany esetében a személyazonosság igazolására elfogadott hatósági igazolványban (személyi igazolvány, útlevél) foglalt névvel betű szerint megegyezően, a névben szereplő ékezetes betűket eredeti írásmódjuk szerint feltüntetve CN és SN mezőkkel (CN = Teljes név = Vezetéknév + Keresztnév, SN = Vezetéknév), az UTF-8 kódolást használva.

Természetes személy alany esetében a tanúsítvány „SubjectAltname” mezőjében szereplő elektronikus levelezési cím struktúrája megfelel az RFC 822 előírásainak.

A tanúsítványok DN mezőiben csak valós nevek szerepelhetnek, álnév használata kizárt.

3.1.3. Nevek egyedisége

A Szolgáltató biztosítja tanúsítványtárában a tulajdonosazonosítók egyediségét, azaz gondoskodik arról, hogy az általa kiadott tanúsítványokban használt megkülönböztetett nevet (DN) sohasem fogja egy másik entitáshoz rendelni. Erről elsődlegesen az Aláíró nevének a névmegadásban való szerepeltetése gondoskodik. A Szolgáltató a név azonosító kiosztásakor ellenőrzi, hogy az adott név szerepel-e egy más személy részére korábban kibocsátott tanúsítványban. Ha szerepel, és a tanúsítvány név azonosítójának egyéb mezői sem biztosítják az egyediséget, akkor a Szolgáltató fenntartja magának a jogot a név olyan megváltoztatására, amely továbbra is jellemző az Aláíróra, de biztosítja a megkülönböztethetőséget.

A nevek kiadására vonatkozó igények teljesítését a Szolgáltató érkezési sorrendben végzi.

3.1.4. Név igénylési viták feloldása

Az Aláírót a tanúsítványban megadott név és a tanúsítvány sorozat száma különbözteti meg egyértelműen a többi Aláírótól.

Az Előfizetőnek álnévre való igényét a regisztrációs űrlapon, az ott rendszeresített módon kell jeleznie.

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

[7] „Information Technology - Open Systems Interconnection - The directory: Overview of concepts, models and services”

3.1.5. Védjegyek elismerésének és hitelesítésének módszere

A tanúsítványkérelemmel az Előfizető kifejezi, hogy a benne foglalt nevek, védjegyek, egyéb adatok nem sértik harmadik fél jogait. Szolgáltatónak nem kötelessége a védjegyek jogos használatának ellenőrzése, és nem vállal közvetítő vagy döntnöki szerepet ilyen jellegű viták feloldásában. Szolgáltató nem garantálja Előfizetők számára védjegyeik feltüntetését a tanúsítványban.

3.1.6. Az aláírás-létrehozó adat birtoklás ellenőrzésének módszere

Az Aláíró számára az aláírás-létrehozó adat és az aláírás-ellenőrző adat (kriptográfiai kulcspár) előállítása a Szolgáltatás keretében a Szolgáltató által történik kiemelt biztonságú környezetben. A kriptográfiai kulcspár a biztonságos aláírás-létrehozó eszközön (BALE; MTT+BALE hitelesítési rend alapján kibocsátott tanúsítványok esetében) vagy a kiemelt biztonságú környezetben (MTT hitelesítési rend alapján kibocsátott tanúsítványok esetében) áll elő, ezért az aláírás-létrehozó adat és az aláírás-ellenőrző adat birtoklásának és egymáshoz tartozásának ellenőrzésére nincs szükség, csupán az aláírás-létrehozó eszköz átvételének igazolása szükséges. Az aláírás-létrehozó eszköz személyes átvételénél az Előfizető aláírásával igazolja az aláírás-létrehozó eszköz és a PIN kód átvételét.

3.1.7. Azonosítás „Személyes” tanúsítvány igénylése esetén

A természetes személy Igénylőnek (Előfizetőnek) ki kell tölteni és alá kell írni a Szolgáltató által biztosított regisztrációs űrlapot.

A természetes személy azonosításához a következő adatokat kéri az Ügyfélkapcsolati Iroda:

a. az Igénylő neve, aláírása
b. az Igénylő okmányszáma (személyi igazolvány vagy útlevél szám)
c. az Igénylő lakcíme
d. az Igénylő e-mail címe

Ezen adatokat személyi igazolvány vagy útlevél illetőleg lakcímigazolvány személyes bemutatásával kell hitelesíteni.

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

Az Előfizető írásbeli nyilatkozatot ad arra vonatkozóan, hogy:

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

A tanúsítvány igénylés nem fogadható el, ha az okmányok személyhez tartozásával, valódiságával vagy érvényességével kapcsolatban kétség merül fel.

3.1.8. Azonosítás „Szervezeti személy” („Munkatársi”) tanúsítvány igénylése esetén

Az igénylő szervezetnek (Előfizetőnek) ki kell tölteni a Szolgáltató által biztosított regisztrációs űrlapot és azt a szervezet képviseletére jogosult vezető tisztségviselő aláírásával kell hitelesíteni.

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

a. az igénylő szervezet neve, székhelye
b. annak a szervezeti egységnek a megnevezése, ahol a szervezeti személy (továbbiakban: Aláíró) dolgozik
c. az Aláíró neve, aláírása
d. az Aláíró beosztása (az előfizető szervezet és szervezeti egység viszonya az Aláíróhoz)
e. az Aláíró személyi igazolvány vagy útlevél száma
f. az Aláíró telefon száma, e-mail címe
g. az Aláírót megbízó dokumentum cégszerűen aláírva (a dokumentum tartalmazza a megbízó szervezet vagy szervezeti egység nevét, e-mail címét, telefon+fax számát)
h. az előfizető szervezet egyértelmű hozzájárulása ahhoz, hogy:
- a tanúsítvány kibocsátásra kerüljön
- a szervezet vagy szervezeti egysége neve a tanúsítvány tulajdonosazonosító mezőjében feltüntetésre kerüljön
- az Aláíró neve a tanúsítvány tulajdonosazonosító mezőjében feltüntetésre kerüljön

- a Szolgáltató a regisztráció során a szervezeti azonosság hitelesítésére elfogad minősített aláírással ellátott elektronikus okiratot is abban az esetben, ha az Előfizetővel ebben előzetesen megegyezik. Ez esetben az Előfizető szervezeti azonosságának hitelesítése, s a szervezeti adatok felvétele a megegyezés során történik, az elektronikus okirat „már csak" az Előfizető hozzájárulását tartalmazza az Aláíró részére történő tanúsítvány kibocsátásához
- az Előfizető kapcsolattartókat nevez meg a Szolgáltató részére, akik aláírási joggal rendelkeznek a tanúsítvány kibocsátását illetően; a Szolgáltató később e személyeknek az aláírását fogadja el bármilyen kérelem vagy bejelentés esetén
- 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. az Aláíró kijelölését engedélyező személy neve (az engedélyezőnek minden esetben a szervezet képviseletére jogosult személynek kell lennie és ezt hiteles dokumentumokkal (pl. aláírási címpéldánnyal) kell igazolni)

b. az engedélyező személy beosztása

c. az engedélyező személy munkahelyi telefonszáma, fax-száma, e-mail címe

Ezen adatokat a következő dokumentumokkal kell hitelesíteni:

a. személyi igazolvány vagy útlevél illetve lakcímigazolvány bemutatása személyesen (Aláíró, Kapcsolattartó)

b. képviseleti megbízás cégszerűen aláírva

c. cégbíróságnál nyilvántartott gazdasági társaságok esetében 30 napnál nem régebbi cégkivonat

d. 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.,

e. állam-, illetve közigazgatási szervezetek esetében az alapító dokumentum közjegyzővel hitelesített másolata, amelyet a szervezet első számú vezetőjének írásos nyilatkozata kísér,

f. 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[8].

Az Ügyfélkapcsolati Iroda szervezeti személy azonosítás-hitelesítése során köteles a tanúsítvány kibocsátását megtagadni, ha

a. a bemutatott okmányok személyhez tartozásával, valódiságával vagy érvényességével kapcsolatban kétsége merül fel

b. a csatolt dokumentumok valódiságával vagy érvényességével kapcsolatban kétsége merül fel

c. a cégnyilvántartással végzett adategyeztetés a bemutatott adatoktól eltérő eredményt ad

d. a szervezet kiléte nem állapítható meg minden kétséget kizáróan

e. nem egyértelmű a szervezet felhatalmazása a tanúsítvány kibocsátására.

3.1.9. Szervezet azonosságának hitelesítése közigazgatásban alkalmazható tanúsítványok igénylése esetén

a) Ha az ***ügyfél*** tanúsítványával kifejezetten jelezni kívánja, hogy ő egy adott szervezethez tartozik, akkor a regisztrációhoz magával kell vinnie az adott szervezet nevében aláírásra jogosult személy által kiállított és aláírt, az adott szervezet nevét is tartalmazó meghatalmazást arra, hogy a szervezet képviseletében a tanúsítványt használja, az aláírásra jogosító aláírási címpéldányt, valamint a szervezet azonosságát is hitelesítő dokumentumot.
A természetes személyt külön is azonosítani kell a 3.1.10. pont szerint.

b) Egy közigazgatási szervet ***képviselő*** természetes személynek a regisztrációhoz magával kell vinnie egy, az adott közigazgatási szerv által kiállított és közokiratba foglalt, a közigazgatási szerv nevét is tartalmazó meghatalmazást arra, hogy a hivatal képviseletében a hitelesítés-szolgáltatónál előforduló ügyekben eljárjon, mely

[8] Eat. 12. § (2) b)

meghatalmazás egyúttal a szervezet azonosságát is hitelesíti.
A természetes személyt külön is azonosítani kell a 3.1.10. pont szerint.

3.1.10.Személy azonosságának hitelesítése közigazgatásban alkalmazható tanúsítványok igénylése esetén

A személy azonosságának hitelesítését a Szolgáltató a 3.1.7 pontban leírtakon felül a következők szerint biztosítja:

a) A regisztrációhoz az igénylőnek személyesen kell megjelennie a Szolgáltató Ügyfélkapcsolati Irodájában. A Szolgáltató eltekint a személyes megjelenéstől, ha az igénylő szervezet felhatalmazott képviselője a szervezet külső helyszínén elvégezte a *b) c)* és *e)* pontok alapján az igénylők azonosítását és regisztrációját és ezt aláírásával igazolja.

b) A regisztráció során az igénylő személyazonosságát a személyazonosság igazolására alkalmas hatósági igazolvány alapján ellenőrizni kell.

c) A regisztráció és a személyazonosság ellenőrzése alapjául szolgáló, rögzítendő adatok helyességét az igénylőnek nyilatkozatban, saját kezű aláírásával ellátva kell igazolnia.

d) A b) pont szerinti hatósági igazolvány azonosító adatait, a megadott adatok egyezését és a hatósági igazolvány érvényességét a Szolgáltató regisztrációs szervezete közhiteles nyilvántartásban ellenőrzi.

e) A regisztrációt végző szervezet regisztrációban részt vevő ügyintézőjének aláírásával kell igazolnia, hogy a hatósági igazolványon szereplő arckép megfeleltethető az igénylő arcának és az igazolványban szereplő aláírás azonos a c) pont szerinti nyilatkozatot igazoló aláírással.

f) Elektronikus aláírás közigazgatási felhasználása esetén a Szolgáltató az ***ügyintéző hatóság*** megkeresésére viszontazonosítást végez, melynek keretében:

- a hatóság a Szolgáltatónak megküldi:
  a) a megadott természetes személyazonosító adatokat (vagy azok egy részét)
  b) a viszontazonosítás alapjául szolgáló ellenőrző adatot (tanúsítványt vagy más, a viszontazonosítást végző szervezetnél az ügyfél azonosítására alkalmas adatot), és
  c) a viszontazonosítási kérést azonosító adatot.
- a Szolgáltató összeveti a megadott természetes személyazonosító adatokat az általa kezelt, beazonosított természetes személyazonosító adatokkal, és válaszként megküldi a viszontazonosítást kérő hatóságnak
  a) az adatok egyezőségének vagy annak hiányának tényét, valamint
  b) a viszontazonosítási kérést azonosító adatot.

g) A Szolgáltató az (f) pont szerinti viszontazonosítást elektronikus úton végzi, s ennek keretében:

- az elektronikus úton küldött viszontazonosítási kérés hitelességének ellenőrzése céljából az ügyintéző hatóság elektronikus aláírását ellenőrzi,
- hiteles viszontazonosítási kérés esetén a választ haladéktalanul megküldi.

h) A ***köztisztviselők*** számára történő tanúsítvány kibocsátást megelőző regisztrációt az alábbiak kezdeményezhetik:

- a hatóságot képviselő természetes személy a Szolgáltató előtt, ha a regisztrációhoz benyújtja a hatóság által kiállított és közokiratba foglalt, a közigazgatási szerv nevét tartalmazó, a hivatal képviseletére feljogosító meghatalmazást;
- a hatóság, ha a regisztrációs szervezet a természetes személy azonosítását külső helyszíni regisztráció útján – szükség szerint a hatóság által kijelölt közigazgatási szerv közreműködésével – végzi el.

i) A h) pont első bekezdése szerinti (a Szolgáltató előtti) regisztráció esetén a Szolgáltató a meghatalmazást kiállító hatóságot – a regisztrációban érintett köztisztviselő adatainak megadása nélkül – a tanúsítvány kibocsátásának tényéről és a hatóság által kiadott meghatalmazásban foglalt iktatószámról értesíti.

3.1.11.Személyi és szervezeti azonosítás időbélyegzés illetve OCSP szolgáltatás igénylés esetén

Időbélyegzés és/vagy OCSP szolgáltatást igényelhet:

a. természetes személy
b. jogi személy (szervezet)

Az időbélyegzés illetve OCSP szolgáltatás igénybe vétele a Szolgáltató és az Előfizető között megkötött szolgáltatási szerződés keretében lehetséges. Ezen szerződés keretében az Előfizető írásbeli nyilatkozatot ad arra vo-

natkozóan, hogy a Szolgáltató nyilvánosan közzétett szabályzataiban részletesen tárgyalt kötelezettségeit, felelősségét és jogait ismeri, s elfogadja azokat.

Az időbélyegzés illetve OCSP szolgáltatás igénybe vételére vonatkozó szerződés megkötése érdekében az Ügyfélkapcsolati Iroda az előfizető személy illetve szervezet azonosítása érdekében a 3.1.12. pontban leírt egyszerűsített azonosítási módot alkalmazza.

Az Ügyfélkapcsolati Iroda az időbélyegzés illetve OCSP szolgáltatási szerződés megkötése során megtagadhatja a szerződés megkötését, ha

a. a bemutatott személyi okmányok személyhez tartozásával, valódiságával vagy érvényességével kapcsolatban kétsége merül fel

b. a megrendelőből a szervezet kiléte nem állapítható meg minden kétséget kizáróan

Az időbélyegzés szolgáltatás igénybe vételekor a Szolgáltató az igénybe vevőnél biztonságos csatornán keresztüli tanúsítvány alapú kliens azonosítást, vagy egyéb, az előfizető egyértelmű azonosítását lehetővé tevő megoldást alkalmaz.

3.1.12.Egyszerűsített azonosítás időbélyegzéshez és OCSP szolgáltatáshoz

Magányszemély előfizető azonosításához személyazonosító igazolvány (személyi igazolvány, útlevél vagy vezetői engedély) és a lakcím kártya bemutatása szükséges.

Szervezeti előfizető azonosításához egy cégszerűen aláírt megrendelő bemutatása szükséges.

4.A működésre vonatkozó követelmények

4.1. Tanúsítványigénylés

A Szolgáltató azt megelőzően, hogy egy Előfizetővel szerződéses kapcsolatot létesít, tájékoztatja az Előfizetőt a tanúsítvány és/vagy az időbélyeg illetve OCSP szolgáltatás használatával kapcsolatos kikötésekről és feltételekről a 2.6.1 pontban megadottak szerint. Ha az Aláíró (alany) nem azonos az Előfizetővel, úgy őt az Előfizető tájékoztatja kötelességeiről.

Tanúsítvány igényléséhez ki kell tölteni a regisztrációs űrlapot és le kell folytatni a 3.1 pontban meghatározott regisztrációs eljárást. Az űrlap nyomtatott vagy elektronikus formában igényelhető az Ügyfélkapcsolati Irodánál, vagy elektronikus formában letölthető a Szolgáltató Internetes honlapjáról.

Az Előfizetői Szerződés aláírásával Előfizető egyúttal nyilatkozik arról is, hogy a Szolgáltató feltételei és kikötései, valamint saját kötelezettségei vonatkozásában tájékoztatást kapott, azokat elfogadja. Az aláírással az Előfizető hozzájárul a szolgáltatások során felhasznált adatoknak a Szolgáltató által történő nyilvántartásba vételéhez, tanúsítványa és az azzal kapcsolatos állapot információk szolgáltatói tanúsítványtárban való közzétételéhez, s ezen adatok harmadik félhez történő továbbításához a Szolgáltató szolgáltatásainak leállítása esetén, illetve egyéb, jogszabályok által meghatározott esetekben. Az Előfizető aláírása igazolja azt is, hogy:

a. vállalja az aláírás-létrehozó eszköz használatát, védelmét
b. garantálja feltüntetett adatainak valódiságát
c. megfizeti a szolgáltatások díját
d. az adatok későbbi változásairól a Szolgáltatót értesíti.

A regisztráció során az Ügyfélkapcsolati Iroda nyilvántartásba veszi az Aláíró azonosítására használt adatokat, beleértve az igazoláshoz használt dokumentumok regisztrációs számát és az azok érvényességével kapcsolatos esetleges korlátozásokat.

A Tájékoztató a szolgáltató internetes honlapján bárki számára elérhető.

4.2. Tanúsítvány kibocsátás

Sikeres regisztráció után az Ügyfélkapcsolati Iroda a tanúsítvány igényt a Regisztrációs Iroda felé továbbítja. A Regisztrációs Iroda a hitelesítés szolgáltatást támogató informatikai rendszerben elindítja a tanúsítvány kibocsátást.

Az elkészült tanúsítvány a következő módon jut el az Előfizetőhöz:

a. az Előfizető, az Aláíró vagy azok képviselője személyesen átveszi az Ügyfélkapcsolati Irodán, vagy
b. az Előfizető letölti a Szolgáltató nyilvános Tanúsítványtárából

4.3. Időbélyegzés

Időbélyegzés szolgáltatás igénylése esetén az Igénylőt tájékoztatni kell az időbélyeg használat módjáról, az azzal járó kötelezettségekről és felelősségről.

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

Az időbélyegzés kérelmek teljesítését a Szolgáltató időbélyegző egysége automatikusan végzi:

a. a kérelmet egy olyan, a szolgáltatás igénybe vétele céljából megkötött szerződésben definiált kommunikációs csatornán keresztül fogadja, amelyen keresztül az időbélyeg kérőt a Szolgáltató rendszere azonosítani tudja,
b. az időbélyeg kérés kiszolgálása az RFC 3161 ajánlás szerinti „application/timestamp-query” MIME-TYPE elküldésére valósul meg.

Az időbélyegzés szolgáltatás az Előfizető részére a szerződéskötést követő 24 órán belül megkezdődik.

Az időbélyegben megadott idő 1 másodpercen belüli pontosságot biztosít. Az időbélyegző egység órájának pontossága folyamatos ellenőrzés alatt áll. Ha ez túllépné a pontossági határt, akkor az ellenőrző program leállítja az időbélyegzés szolgáltatást, és minden további kérésre a hiba kijavításáig hibaüzenetet küld a felhasználók felé. A szolgáltatás akkor indul újra, ha az időszinkron helyreállt és az egy másodperces pontossági határ teljesül. Az időszinkron helyreállítását a Szolgáltató húsz percen belül biztosítja.

4.4. OCSP szolgáltatás

OCSP szolgáltatás igénylése esetén az Igénylőt tájékoztatni kell a használat módjáról, az azzal járó kötelezettségekről és felelősségről.

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

Az OCSP kérelmek teljesítését a Szolgáltató OCSP egysége automatikusan végzi:

a. a kérelmet egy olyan, a szolgáltatás igénybe vétele céljából megkötött szerződésben definiált kommunikációs csatornán keresztül fogadja, amelyen keresztül az OCSP válasz kérőt a Szolgáltató rendszere azonosítani tudja,

b. az OCSP kérés kiszolgálása az RFC 2560 ajánlás szerinti „application/ocsp-request" MIME-TYPE elküldésére valósul meg.

Az OCSP szolgáltatás az Előfizető részére a szerződéskötést követő 24 órán belül megkezdődik.

Az OCSP válaszban megadott idő 1 másodpercen belüli pontosságot biztosít. Az OCSP válaszadó egység órájának pontossága folyamatos ellenőrzés alatt áll.

4.5. Tanúsítvány elfogadás

A tanúsítvány elfogadása az Előfizető részéről az átvétellel történik meg.

Az Előfizető (Aláíró) a tanúsítvány használatba vétele előtt köteles ellenőrizni a tanúsítvány adatainak helyességét.

Az aláírás-létrehozó adat használatba vétele előtt az Előfizető (Aláíró) köteles ellenőrizni a tanúsítvány adatainak helyességét és visszaigazolni a tanúsítvány átvételét. Amennyiben bármilyen rendellenességet talál, az aláírás-létrehozó adatot nem használhatja fel, hanem azonnal intézkednie kell a tanúsítvány visszavonására.

A visszaigazolás egyben a Hitelesítési rend, a Szolgáltatási szabályzat és az Általános szerződési feltételek elfogadását is jelenti.

4.6. Érvényes tanúsítvány megújítása (tanúsítvány frissítése)

Tanúsítványfrissítés során a Szolgáltató a tanúsítványban az Aláíró változatlan nyilvános kulcsát és változatlan egyéb adatait hitelesíti új érvényességi időtartamra.

Előfizetői tanúsítvány megújítása akkor lehetséges, ha:

a. a tanúsítvány nem szerepel a Visszavont Tanúsítványok Listájában

b. a tanúsítványban rögzített adatok érvényességéről és változatlanságáról az Előfizető írásban nyilatkozik.

A Szolgáltató az Előfizető nyilatkozata alapján adatai érvényességéről és változatlanságáról az illetékes hatóságokkal egyeztetést végezhet.

Ha a feltételek valamelyike nem teljesül, új tanúsítványt kell igényelni a regisztrációs eljárás újbóli végrehajtásával.

A Szolgáltató a tanúsítvány megújítás szükségességéről a lejárat előtt értesítést küld az Előfizetőnek.

4.7. Kulcscsere

A kulcscsere az a folyamat, amelynek során a Szolgáltató úgy bocsát ki egy megújított tanúsítványt, hogy abban az eredeti tanúsítvány alanyra vonatkozó adatai közül csak a nyilvános kulcs kerül lecserélésre.

Kulcscserére a következő esetekben lehet szükség:

- a tanúsítvány valamilyen okból visszavonásra került,

- a tanúsítvány lejárt,

- a magánkulcsot tartalmazó biztonságos aláírás-létrehozó eszköz megsérült és nem használható

A kulcscserét az Előfizető kezdeményezheti. Kulcscsere esetén a Szolgáltató lefolytatja a 3.1. pontban rögzített regisztrációs eljárást. A megújított tanúsítvány kibocsátása és publikálása megegyezik az új tanúsítványra vonatkozó eljárásokkal.

4.8. Tanúsítvány-módosítás

A tanúsítvány-módosítás az a folyamat, amelynek során a hitelesítés-szolgáltató úgy bocsát ki egy módosított tanúsítványt, hogy abban az eredeti tanúsítvány alanyra vonatkozó adatai – a nyilvános kulcs kivételével – változnak, és a tanúsítvány az új adatokkal, valamint a régi nyilvános kulccsal kerül kiadásra.

Tanúsítvány-módosításra akkor lehet szükség, ha a tanúsítvány alanyra vonatkozó adatai – a nyilvános kulcs kivételével – megváltoztak.

A tanúsítvány-módosítást az Előfizető kezdeményezheti.

A kérelem benyújtásakor a Szolgáltató ellenőrzi a tanúsítvány létezését és érvényességét, valamint az alany azonosságának és jellemzőinek igazolására használt információk érvényességét a 3.1. pontban rögzített regisztráci-

ós eljárás szerint.

A módosított tanúsítvány kibocsátása és publikálása megegyezik az új tanúsítványra vonatkozó eljárásokkal.

A Szolgáltató a módosítandó tanúsítványt a módosított tanúsítvány kibocsátása előtt visszavonja.

4.9. Érvénytelen tanúsítvány megújítása

Tanúsítvány megújítása nem lehetséges, ha a tanúsítvány érvényessége lejárt, vagy ha a tanúsítvány visszavont állapotban van. Ezen esetekben új tanúsítványt kell igényelni a regisztrációs eljárás újbóli végrehajtásával.

4.10. Felfüggesztés és visszavonás kérés

A Szolgáltató gondoskodik arról, hogy az általa kibocsátott tanúsítványok érvényességét az Előfizető vagy az Aláíró kérésére felfüggessze vagy a tanúsítványt visszavonja. Ennek érdekében a Szolgáltató a 4.11 pontban rögzíti a tanúsítványok visszavonásának és felfüggesztésének eljárásait.

4.11. Tanúsítvány felfüggesztés és visszavonás

A Szolgáltató a tanúsítványok érvényességének kezelésére mind tanúsítvány visszavonási, mind tanúsítvány felfüggesztési szolgáltatást nyújt. A tanúsítvány visszavonása a tanúsítvány állapotát végérvényesen érvénytelenre állítja. Felfüggesztés esetén a tanúsítvány csak rövid, átmeneti időszakra lesz érvénytelen. A tanúsítvány felfüggesztett állapotban csak ideiglenesen lehet, az engedélyezett időtartam (lásd 4.11.7 pont) után állapotát újra érvényesre kell állítani, vagy a tanúsítványt vissza kell vonni.

A felfüggesztési és visszavonási kérelmeket az Ügyfélkapcsolati irodák fogadják nyitvatartási időben. A felfüggesztési kérelmek fogadását és azoknak a sikeres ellenőrzés utáni végrehajtását a Szolgáltató Ügyfélszolgálatán keresztül is biztosítja, a nap 24 órájában, folyamatos rendelkezésre állással.

4.11.1. Visszavonáshoz/felfüggesztéshez vezető körülmények

A Szolgáltató felfüggeszti vagy visszavonja a tanúsítványt ha:

- *a.* az Előfizető vagy az Aláíró ezt kéri
- *b.* megalapozottan feltételezhető, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak, azok használata jogszerűtlen, vagy az aláírás-létrehozó adat nem az Aláíró kizárólagos birtokában van
- *c.* a Szolgáltató és az Előfizető között a szerződés megszűnt
- *d.* a Nemzeti Hírközlési Hatóság jogerős és végrehajtható határozatában így rendelkezik
- *e.* a Szolgáltató a szolgáltatással kapcsolatos rendellenességről vesz tudomást és a rendellenesség az érvényes szabályok szerint nem orvosolható
- *f.* a Szolgáltató a tevékenységét befejezte

Az Előfizető vagy az Aláíró a következő körülmények fennállása esetén kezdeményezheti a visszavonást/felfüggesztést:

- *a.* a magánkulcs kompromittálódása, vagy annak gyanúja
- *b.* az aláírás-létrehozó eszköz elvesztése, eltulajdonítása, megrongálódása
- *c.* az aláírás-létrehozó eszközt védő aktivizáló adat (PIN kód) kompromittálódása, vagy annak gyanúja
- *d.* a tanúsítványban feltűntetett hibás adatok
- *e.* az Előfizető tanúsítványban feltűntetett adatainak megváltozása
- *f.* az Aláíró tanúsítványban feltűntetett adatainak megváltozása
- *g.* a tanúsítványban feltűntetett Aláíró és szervezet kapcsolatának megváltozása vagy megszűnése[9].

A visszavonási/felfüggesztési kérelmet a Szolgáltató mérlegelés nélkül teljesíti, ha azt az Előfizető vagy az Aláíró kéri.

A felfüggesztés/visszavonás a Szolgáltató kezdeményezése alapján a következő esetekben történhet:

- *a.* a tanúsítvány felfüggesztési idejének lejárata
- *b.* amennyiben a törvény erre kötelezi
- *c.* az ÁSZF-M vagy az Előfizetői Szerződés megszegése az Előfizető és/vagy az Aláíró által
- *d.* az Előfizető és/vagy az Aláíró kötelezettségeinek be nem tartása
- *e.* az Előfizetői szerződés megszűnése
- *f.* a Szolgáltató tudomására jutott tény, vagy alapos gyanú, a regisztrációs adatok valótlanságáról

[9] Eat. 10. § (3)

g. a tanúsítványban feltűntetett kibocsátó adatok megváltozása

h. a hitelesítési szolgáltatás megszűnése

i. a Szolgáltató valamely magánkulcsának kompromittálódása miatt

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 érdekében.

4.11.2.Visszavonás/felfüggesztés kérelmezése

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

Felfüggesztési kérelem benyújtható személyesen vagy írásban a Szolgáltató Ügyfélkapcsolati Irodájánál. A bejelentő akadályoztatása vagy azonnali intézkedés szükségesége esetén a tanúsítvány felfüggesztése telefonon vagy elektronikusan aláírt e-mail-ben is kérhető az Ügyfélszolgálaton. A tanúsítvány visszavonására az ettől számított 5 napon belül kell intézkedni.

Minősített tanúsítványra a visszavonási kérelmet a Szogáltató csak a következő formában fogadja el:

a. személyesen az Ügyfélkapcsolati Irodánál

b. közjegyzővel hitelesített írásbeli nyilatkozatban

c. az Aláíró által az Ügyfélkapcsolati Irodához címzett, minősített aláírással hitelesített elektronikus dokumentumban.

A visszavonási kérelemnek a következő adatokat kell tartalmaznia:

a. a tanúsítvány sorszáma, vagy egyéb olyan adatok, amely alapján a Szolgáltató rendszerében a tanúsítvány egyértelműen azonosítható

b. a visszavonást kérő megnevezése, azonosító adatai

c. a visszavonást kérő e-mail címe (ha van)

d. a visszavonáshoz vezető körülmények.

A felfüggesztési kérelemnek a visszavonási kérelemmel megegyező adatokat (illetve a Szolgáltató ügyfélszolgálatán keresztül történő bejelentés esetén azokon túlmenően a felfüggesztési jelszót) kell tartalmaznia.

4.11.3.A visszavonási kérelemre vonatkozó kivárási idő

a) A Szolgáltató a visszavonási, illetve felfüggesztési kérelem fogadásától számított 3 órán belül dönt a kérelem érvényességéről (elbírálja a kérelmező jogosultságát), és érvényes kérelem esetén a visszavonási állapot megváltozását a nyilvántartásában átvezeti.

b) Ha a Szolgáltató a visszavonási kérelem érvényességéről 3 órán belül nem tud kétséget kizáróan meggyőződni, akkor a tanúsítványt nem visszavonja, hanem felfüggeszti, és a visszavonást később – a kérelmező hiteles azonosítását követően végzi el.

c) Az a) vagy a b) pontban foglaltak teljesítését követően a Szolgáltató a visszavonási (illetve felfüggesztési) kérelem szerint módosított visszavonási állapotot 1 órán belül közzéteszi.

4.11.4.Visszavonási/felfüggesztési kérelemre vonatkozó türelmi idő

A visszavonási/felfüggesztési kérelem esetén a bejelentési kötelezettség azonnali, a Szolgáltató ennek végrehajtását soron kívül végrehajtja a kérelem elfogadása után. A legnagyobb késedelem a visszavonási/felfüggesztési kérelem elfogadása és a visszavonási/felfüggesztési állapot közzététele között: 1 óra.

A Szolgáltató akkor tekinti a visszavonási/felfüggesztési kérelmet elfogadottnak, ha annak jogosságáról meggyőződött. A visszavonási/felfüggesztési kérelemre vonatkozó türelmi idő 3 óra. Ha a Szolgáltató ezen időn belül sem tud a kérelem jogosságáról meggyőződni, akkor a felfüggesztési/visszavonási kérelmet visszautasítja.

Visszavont/felfüggesztett tanúsítványt joghatályosan nem lehet felhasználni.

A Szolgáltatót és az Előfizetőt érintő felelősségi szabályok:

a. A visszavonási/felfüggesztési kérelem bejelentésének a Szolgáltatóhoz történő megérkezéséig az Előfizető felelős a felmerülő károkért.

b. A visszavonási/felfüggesztési kérelem elfogadásától a visszavonás/felfüggesztés tényének a Visszavont Tanúsítványok Listájában való megjelenésig a Szolgáltató felelős a felmerülő károkért. Ez alól kivételt képez a bizonyíthatóan csalárd szándékkal történt visszavonás/felfüggesztés kérés, amely esetben a felmerülő károkért a Szolgáltató nem vállal felelősséget.

c. A felfüggesztett/visszavont tanúsítványnak a Visszavont Tanúsítványok Listájában való megjelenése után az Érintett fél felelős a felmerülő károkért.

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

4.11.5.Visszavonási eljárás

A visszavonási eljárás első lépéseként a Szolgáltató azonosítja a bejelentőt, majd mérlegeli a visszavonási okokat.

Ha a visszavonási okok megalapozottak és az ellenőrzések sikeresek, a Szolgáltató elvégzi a tanúsítvány visszavonását.

Ha a visszavonási okok nem megalapozottak, az adatok helytelenek, vagy a kérelmező személye nem állapítható meg kellő bizonyossággal vagy a kérelmezőnek a Szolgáltató információi alapján nincs joga a tanúsítvány visszavonatására, akkor a Szolgáltató a visszavonási kérelmet visszautasítja.

Szolgáltató a visszavonás megtörténtéről vagy visszautasításáról értesíti az Aláírót, az Előfizetőt és a visszavonás kérelmezőjét.

A visszavont tanúsítvány a visszavonási eljárás befejezése után haladéktalanul bekerül a Visszavont Tanúsítványok Listájába.

4.11.6.Felfüggesztési eljárás

A felfüggesztési eljárás első lépéseként a Szolgáltató azonosítja a bejelentőt, majd mérlegeli a felfüggesztési okokat:

a. ha a felfüggesztési kérelmet az Előfizető terjesztette be, az Előfizető azonosítása után a Szolgáltatónak nincs mérlegelési joga a felfüggesztés tekintetében

b. ha a felfüggesztési okok megalapozottak és az ellenőrzések sikeresek, a Szolgáltató elvégzi a tanúsítvány felfüggesztését

c. ha a felfüggesztési okok nem megalapozottak, az adatok helytelenek, vagy a kérelmező személye nem állapítható meg kellő bizonyossággal vagy a kérelmezőnek a Szolgáltató információi alapján nincs joga a tanúsítvány felfüggesztésére, akkor a Szolgáltató a felfüggesztési kérelmet visszautasítja

Szolgáltató a felfüggesztés megtörténtéről vagy visszautasításáról értesíti az Aláírót, az Előfizetőt és a felfüggesztés kérelmezőjét.

A felfüggesztett tanúsítvány a felfüggesztési eljárás befejezése után azonnal bekerül a Visszavont Tanúsítványok Listájába.

4.11.7.A felfüggesztett állapotra vonatkozó korlátozások

Tanúsítvány felfüggesztett állapotban legfeljebb 5 naptári napig lehet.

Ha a felfüggesztést az Előfizető vagy az Aláíró kérte, akkor a kérelmezőnek ezen időszak alatt értesítenie kell a Szolgáltatót a tanúsítvány érvényesítése vagy visszavonása felől. Ha ilyen értesítés nem történik Szolgáltató a tanúsítványt visszavonja.

Ha a felfüggesztésről a Szolgáltató határozott, akkor 5 napon belül dönt a tanúsítvány visszavonásáról is. Amennyiben Szolgáltató nem képes ezen időszak alatt a körülmények kivizsgálására, akkor a tanúsítványt visszavonja, valamint az Előfizető igénye estén részére térítésmentesen új tanúsítványt bocsát ki.

A felfüggesztés megszüntetése a felfüggesztési időszak vége előtt is kérhető. A felfüggesztés megszűntetésének eredménye a tanúsítvány újraérvényesítése vagy visszavonása.

Az újraérvényesítés feltételei a következők:

a. az újraérvényesítést csak az Előfizető vagy annak a regisztráció során nyilvántartásba vett képviselője kérheti

b. az újraérvényesítést kérő személyt azonosítani kell.

Az újraérvényesítés kéréséhez a következő adatokat kell megadni:

a. a felfüggesztett tanúsítvány sorszáma

b. a felfüggesztés megszüntetést kérő személy azonosító adatai

c. a felfüggesztés megszüntetésének oka

4.11.8.Visszavont Tanúsítványok Listája (CRL) és kibocsátásának gyakorisága

A Visszavont Tanúsítványok Listájába a visszavont és felfüggesztett tanúsítványok kerülnek. A felfüggesztett tanúsítványok az újraérvényesítés hatására kerülhetnek ki a listából. A Szolgáltató a lejárt tanúsítványokat a listából törli.

A Szolgáltató által kezelt Visszavont Tanúsítványok Listájának érvényességi ideje 24 óra. Szolgáltató legkésőbb a lista érvényességi idejének lejártakor új listát bocsát ki, új érvényességi idővel.

A Szolgáltató egy-egy tanúsítvány felfüggesztését, visszavonását illetve újraérvényesítését követően 1 órán belül új visszavonási listát tesz közzé.

4.11.9.Visszavont Tanúsítványok Listája ellenőrzése

A Visszavont Tanúsítványok Listája ellenőrzése az érintett felek felelőssége a tanúsítványok elfogadását megelőzően. A tanúsítványhoz tartozó visszavonási lista elérhetőségét a tanúsítvány tartalmazza. A lista ellenőrzésének arra kell vonatkozni, hogy a kérdéses tanúsítványt a lista tartalmazza-e (és ha igen, milyen időponttól), a lista hiteles és sértetlen, s a kérdéses tranzakció szempontjából időben releváns-e.

A tanúsítvány visszavonási listában a Szolgáltató által közzétett visszavont, vagy felfüggesztett tanúsítvány elfogadásából keletkező bárminemű kár Érintett felet terheli.

4.11.10.Visszavonási állapot közlés más formái

A Szolgáltató a Visszavont Tanúsítványok Listája mellett online visszavonási információs (OCSP) szolgáltatást nyújt. Az OCSP szolgáltatás nyújtása elsősorban a 4.4 és 3.1.11 pontokban foglaltaknak megfelelően történik.

4.11.11.Intézkedések magánkulcs kompromittálódás esetén

Az aláírás-létrehozó adat tényleges vagy vélelmezett kompromittálódása esetén a tanúsítvány visszavonásáról illetve felfüggesztéséről azonnal intézkedni kell. Alapos gyanú esetén az aláírás-létrehozó adat használatát azonnal be kell szüntetni.

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

4.12. Biztonsági audit eljárások

A Szolgáltató hitelesítés-szolgáltatását és időbélyegzését támogató informatikai rendszerének biztonsági naplózását és annak auditálását a jelen HSZSZ-M mellett a PKI szolgáltatások biztonsági szabályzata részletezi.

4.12.1.Naplózott esemény típusok

A Szolgáltató gondoskodik arról, hogy az általa kibocsátott tanúsítványokra vonatkozó minden lényeges adat rögzítésre és megőrzésre kerüljön, különösen jogi eljárásokhoz bizonyíték nyújtása érdekében.

A tanúsítvány előállítással kapcsolatosan a Szolgáltató naplóz minden a rendszerrel és a szolgáltatás nyújtásával kapcsolatos eseményt, különösen:

- *a.* a szolgáltatói tanúsítványok életciklusával kapcsolatos összes eseményt
- *b.* az előfizetői tanúsítványokat aláíró infrastruktúrális és ellenőrző kulcsok tanúsítványainak életciklusával kapcsolatos összes eseményt, ezen belül különösen az előfizetői tanúsítványok előállítási és megújítási igény-benyújtási időpontját, valamint az igények teljesítésének időpontját

Az Előfizetők biztonságos aláírás-létrehozó eszközzel való ellátásával kapcsolatosan a Szolgáltató naplóz minden általa gondozott kulcs életciklusával kapcsolatos eseményt és a biztonságos aláírás-létrehozó eszközök megszemélyesítésével kapcsolatos valamennyi eseményt.

A visszavonás kezeléssel kapcsolatosan a Szolgáltató gondoskodik a kérések, valamint az ezek következtében előállt tevékenységek naplózásáról.

Az időbélyegzéssel kapcsolatosan naplóz minden a rendszerrel és a szolgáltatás nyújtásával kapcsolatos eseményt, különösen:

- *a.* az időbélyegzés szolgáltatás fő lépései, a kérelemtől az időbélyeg válasz elküldésig
- *b.* az időbélyeget aláíró kulcsok életciklusában bekövetkező eseményeket (generálás, használat, visszavonás, megsemmisítés)
- *c.* az időbélyeget aláíró kulcsok tanúsítványa életciklusában bekövetkező eseményeket (kiadás, használat, visszavonás)

Az OCSP szolgáltatással kapcsolatosan naplóz minden a rendszerrel és a szolgáltatás nyújtásával kapcsolatos eseményt, különösen:

a. az OCSP szolgáltatás fő lépései, a kérelemtől az OCSP válasz elküldésig
b. az OCSP válaszokat aláíró kulcsok életciklusában bekövetkező eseményeket (generálás, használat, visszavonás, megsemmisítés)
c. az OCSP válasz aláíró kulcsok tanúsítványa életciklusában bekövetkező eseményeket (kiadás, használat, visszavonás)

A hitelesítés-szolgáltatást támogató informatikai rendszer biztonságával kapcsolatosan naplózza:

a. a naplózási funkció elindításával és leállításával
b. a naplózási paraméterek megváltoztatásával
c. a naplózás tárolásával kapcsolatos hibákkal
d. a napló adatok integritásának megsértésével
e. a hitelesítés-szolgáltatást támogató informatikai rendszerhez történő bármely hozzáférési kísérlettel kapcsolatos eseményeket

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

A pontos időt a Szolgáltató időbélyegző egysége biztosítja.

A hitelesítés szolgáltatást támogató informatikai rendszer operációs rendszerére, illetve a rendszer többi elemére vonatkozóan a biztonsági szabályzatban meghatározott események kerülnek naplózásra.

4.12.2.Napló adatok védelme

A Szolgáltató a napló adatokat fokozott biztonságú fizikai környezetben menti el, a mentett állományokat időbélyeggel ellátott elektronikus aláírással hitelesíti és védett környezetben tárolja. A naplók olvasása hozzáférési jogosultsághoz kötött.

A Szolgáltató biztosítja naplóállományok bizalmasságát és sértetlenségét.

4.12.3.Napló adatok feldolgozása

A PKI alkalmazás, az időbélyegzés alkalmazás és az operációs rendszerek biztonsági esemény és audit naplóinak operatív ellenőrzését csak a rendszervizsgálók végezhetik és csak olvasási jogosultsággal. A rendszervizsgálók feladata az alkalmazásokon és operációs rendszereken kívüli, de a PKI rendszer részét képző szoftver elemek (hálózat, tűzfalak, betörés detektor) naplóinak ellenőrzése is.

4.12.4.Napló adatok tárolása

A napló adatokat a Szolgáltató archiválja (lásd: 4.13.3 pont).

4.12.5.Rendkívüli eseményekről történő értesítés

A hitelesítés-szolgáltatást támogató informatikai rendszerre, annak fizikai és személyi környezetére kiható súlyos üzemzavari és katasztrófa események megelőzéséről, kezeléséről, az érintettek értesítéséről és a rendszer visszaállításáról részletesen a Szolgáltató Üzletmenet-folytonossági Terve intézkedik. Az Üzletmenet-folytonossági Tervben az üzletmenetet veszélyeztető, sértő, illetve azt leállító események súlyossági osztályokba vannak sorolva. A Terv részletesen szabályozza a Hitelesítő Központok saját aláírás-létrehozó adatainak, aktiváló adatainak és az időbélyegek aláíró kulcsának kompromittálódása esetén elvégzendő teendőket.

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

4.13. Adatarchiválás

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

4.13.1.A tárolt adatok típusai

A Szolgáltató gondoskodik arról, hogy megőrzésre kerüljön a regisztráció során felvett összes információ, beleértve az alábbiakat is:

a. az Igénylő által a regisztráció támogatása céljából benyújtott dokumentum(ok) típusa
b. az azonosító dokumentumok egyedi azonosító adatai (például az Igénylő jogosítvány száma)
c. az Igénylő és azonosító dokumentumok (beleértve az aláírt, az Előfizetővel kötött megállapodást másolatainak tárolási helyszíne)
d. az Előfizetővel kötött megállapodás esetleges egyedi választásai

e. a kérelmet elfogadó regisztrációs felügyelő (RO) azonosítója

f. a fogadó Hitelesítő Központ és/vagy a küldő regisztrációs felügyelő (RO) azonosítója, amennyiben ez értelmezhető

A 4.12.1 pontban felsorolt összes esemény, illetve napló típus.

4.13.2.Az archívum gyűjtési rendszere

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

4.13.3.Az archívum megőrzési időtartama

A Szolgáltató 4.13.1 pontban megnevezett nyilvántartásokat és a 4.12.1 pontban megnevezett naplókat az Eat. 9. § (7) bekezdése alapján és a 3/2005. (III. 18) IHM rendelettel összhangban a keletkezésüktől számított 10 évig, illetve jogi eljárásban a tanúsítványokon keresztül történő bizonyításhoz szükséges ideig megőrzi.

4.13.4.Az archívum védelme

A Szolgáltató az archívumában és a Biztonsági Adattárában olyan fizikai védelmet biztosít, amely fenntartja a tanúsítványokra és az időbélyegzésre vonatkozó aktuális és archivált adatok bizalmasságát és sértetlenségét. A Szolgáltató az archivált adatokat legalább fokozott biztonságú elektronikus aláírással és időbélyegzővel látja el.

4.13.5.Az archívum hozzáférését és ellenőrzését végző eljárások

A Szolgáltató az archívumhoz Ügyfélkapcsolati Irodáján keresztül biztosít hozzáférést és értelmezhetőséget. A jogosultságot és a hozzáférést a Szolgáltató minden esetben ellenőrzi és naplózza. A Szolgáltató biztosítja az archivált adatok megjelenítéséhez (olvasásához) szükséges eszközt.

4.14. A folyamatos üzemmenet biztosítása (katasztrófa elhárítás)

A Szolgáltató olyan megbízható rendszert működtet, amely a rendszerben bekövetkezett hiba esetén is biztosítja a szolgáltatások elérhetőségét.

A Szolgáltató gondoskodik arról, hogy rendkívüli üzemeltetési helyzet esetén (súlyos üzemzavar vagy katasztrófa, beleértve a saját aláírás-létrehozó magánkulcsának kompromittálódását, illetve kritikus szoftver/hardver komponenseinek meghibásodását is) a rendszerüzemeltetés a lehető legrövidebb időn belül helyreálljon.

A Szolgáltató rendkívüli üzemeltetési helyzet esetén is gondoskodik a tanúsítvány visszavonás kezelés és visszavonási állapot közzététel, valamint az időbélyegzés szolgáltatások fenntartásáról (lásd: 2.1.1 fejezet 6. pont).

A rendkívüli üzemeltetési helyzetek kezelésére a Szolgáltató rendelkezik biztonsági mentésekkel, tartalékolt műszaki megoldásokkal és eljárásokkal. A megelőzőzésre és rendkívüli üzemeltetési helyzetekre érvényes intézkedéseket a Szolgáltató Üzletmenet-folytonossági Terve tartalmazza.

A rendkívüli üzemeltetési helyzetekben a Szolgáltató eseménynaplót vezet.

4.14.1.Biztonsági képesség rendkívüli üzemeltetési helyzetben

Súlyos üzemzavar, természeti vagy más egyéb katasztrófát követően a Szolgáltató életbe lépteti Üzletmenet-folytonossági Tervében megtervezett eljárásait annak érdekében, hogy az üzemeltetés helyreálljon az Üzletmenet-folytonossági Tervben megjelölt időn belül.

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

4.14.2.Minimális szolgáltatás rendkívüli üzemeltetési helyzetben

A Szolgáltató rendkívüli üzemeltetési helyzetben is biztosítja az időbélyegzés szolgáltatást, Tanúsítványtárának elérhetőségét, a tanúsítványok felfüggesztésére és visszavonására vonatkozó kérelmek fogadását és teljesítését, valamint a visszavonási/felfüggesztési állapot közzétételét a Visszavont Tanúsítványok Listájában.

Rendkívüli üzemeltetési helyzetben a Szolgáltató minden egyéb szolgáltatást szüneteltet.

4.14.3.Üzletmenet-folytonossági Terv

A Szolgáltató rendelkezik Üzletmenet-folytonossági Tervvel, amely részletes intézkedési forgatókönyveket tartalmaz a súlyos üzemzavarok vagy katasztrófa események kezelésére. Ez a dokumentum biztonsági okokból nem nyilvános.

4.15. A hitelesítés-szolgáltatási tevékenység megszüntetése

A Szolgáltató a tervezett megszűnés előtt tárgyalásokat kezd más szolgáltatókkal a szolgáltatások átvételéről. A tárgyalások eredményéről tájékoztatja a felhasználói közösséget.

A Szolgáltató gondoskodik a szolgáltatásainak megszüntetéséből fakadó, a felhasználói közösséget érintő zavarok minimalizálásáról. Különösképpen gondoskodik az időbélyegzés, a tanúsítvány visszavonás kezelés és közzététel szolgáltatások folyamatos fenntartásáról.

Ennek érdekében a Szolgáltató mielőtt hitelesítés-szolgáltatási tevékenységét leállítja:

a. legalább 60 nappal korábban értesíti a Nemzeti Hírközlési Hatóságot és Internetes honlapján tájékoztatja a felhasználói közösség tagjait

b. megszűnteti a tanúsítványok kibocsátási folyamatában a nevében eljáró alvállalkozások összes felhatalmazását

c. megteszi a szükséges lépéseket, hogy a regisztrációs adatok és az eseménynapló archívumok fenntartására vonatkozó kötelezettségeket átruházza

A bejelentéssel egyidejűleg a Szolgáltató leállítja:

a. a tanúsítvány előállítás és kibocsátás szolgáltatást (ezen belül a tanúsítvány megújítását)

b. az OCSP szolgáltatást

c. a biztonságos aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatást.

Szolgáltató a tervezett megszűnés előtt 20 nappal intézkedik az előfizetői tanúsítványok és szolgáltatói tanúsítványai visszavonásáról.

Ezzel egyidejűleg leállítja az időbélyegzést és a visszavonás kezelési szolgáltatását.

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

Eljárás Regisztrációs Iroda megszűnése esetén:

a. A Regisztrációs Iroda megszűnése előtt 60 nappal értesíti azon Előfizetőket, akik a megszűnő Regisztrációs Irodánál kötöttek szerződést és a Szolgáltató által kibocsátott érvényes tanúsítvánnyal rendelkeznek.

b. A Regisztrációs Iroda megszűnéséről a felhasználói közösség tagjait Szolgáltató a web oldalain történő közzététel útján tájékoztatja.

5.Fizikai, eljárásrendi, és humán biztonsági szabályozások

A Szolgáltató az elfogadott szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket és az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmazza. Ezen belül:

a. A Szolgáltató kockázat elemzést végzett üzleti kockázatainak felmérésére, valamint a szükséges biztonsági követelmények és működési eljárások meghatározására

b. A Szolgáltató a szervezetén belüli biztonságkezeléshez szükséges informatika biztonsági infrastruktúrát folyamatosan fenntartja. A biztonság szintjére hatást gyakorló bárminemű változtatást a Szolgáltató vezetősége hagy jóvá

c. A Szolgáltató megvalósította és folyamatosan fenntartja az aláírás-hitelesítési, időbélyegzési és OCSP szolgáltatási szolgáltatásokat nyújtó eszközök, rendszerek és informatikai értékek biztonsági ellenőrzéseit és üzemeltetési eljárásait.

d. A Szolgáltató gondoskodik az informatikai biztonság fenntartásáról azokban az esetekben is, amikor az elektronikus aláírással, időbélyegzéssel és OCSP szolgáltatással kapcsolatos szolgáltatások egyes funkcióira vonatkozó felelősségek más szervezethez kerülnek kiadásra.

A Szolgáltató biztonsági műveletei közé az alábbiak tartoznak:

a. üzemeltetési eljárások és felelősségek
b. ellenőrzési eljárások
c. biztonsági rendszerek és eljárások tervezése, elfogadása és működtetése
d. erőforrás gazdálkodás
e. hálózat menedzselés
f. a biztonsági naplók aktív felügyelete, eseményelemzések és nyomkövetések
g. adathordozó eszközök kezelése és biztonsága
h. rendszerkarbantartás

E felelősségeket a Szolgáltató biztonsági műveletei kezelik, és azokat a 3/2005. (III. 18) IHM rendelet 20.§-21.§-nak megfelelő, megbízható és szakértő üzemeltető személyzet hajthatja végre.

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

A Szolgáltató fizikai, eljárásrendi (adminisztratív) és humán biztonsági szabályozásait a PKI Szolgáltatások Biztonsági Szabályzata tartalmazza részletesen. Ez a szabályzat biztonsági okokból nem nyilvános.

A szolgáltatásokat támogató informatikai rendszer, annak személyi és fizikai környezete a MeH ITB 12. ajánlás szerint a fokozott biztonsági osztályba tartozik, amely egyértelműen meghatározza a Hitelesítő Központok és a Regisztrációs Iroda informatikai rendszereinek, valamint a hitelesítés-szolgáltatással kapcsolatos valamennyi szolgáltatás személyi és fizikai környezetének biztonsági követelményeit.

A következő pontok csak a vonatkozó lényeges intézkedéseket tartalmazzák.

5.1. Fizikai biztonsági szabályozások

5.1.1. Hitelesítő Központok

A hitelesítő központok legmagasabb védelmi szintet képező objektuma a Bizalmi Központ, amely a biztonsági szempontból legkritikusabb hardver/szoftver egységeket tartalmazza. A Bizalmi Központban történik a kulcspárok és a tanúsítványok előállítása, a kulcspárok elhelyezése az aláírás-létrehozó eszközre és az aláírás-létrehozó eszközök megszemélyesítése. A Bizalmi Központ védelme kielégíti a MeH ITB 12. ajánlása szerinti fokozott biztonsági osztály követelményeit.

5.1.2. Regisztrációs Iroda

A regisztrációs iroda a Bizalmi Központon belül van kialakítva, itt találhatók a regisztrációs munkahelyek és munkaállomások. A Regisztrációs Iroda védelme kielégíti a MeH ITB 12. ajánlása szerinti fokozott biztonsági osztály követelményeit.

5.2. Eljárásrendi szabályozások

A Szolgáltató eljárásrendi szabályait a következő szabályzatok tartalmazzák:

a. a Szolgáltató Szervezeti és Működési Szabályzata, amely részletesen meghatározza a Szolgáltató szervezeti felépítését, azon belül az egyes munkaköröket és az azokhoz kapcsolt feladat-, felelősség és hatásköröket,

b. a jelen Szolgáltatási Szabályzat,

c. a PKI Szolgáltatások Biztonsági Szabályzata, amely részletesen szabályozza az adatokhoz és az informatikai rendszerekhez, valamint a személyi és a fizikai környezethez kapcsolódó biztonsági szabályokat.

5.3. Humán szabályozások

5.3.1. Bizalmi munkakörök

A 3/2005. (III. 18.) IHM rendelet 2 § nevesíti a minősített hitelesítés-szolgáltatáshoz kapcsolódó bizalmi munkaköröket:

a. a Szolgáltató informatikai rendszeréért általánosan felelős vezető,

b. biztonsági tisztségviselő,

c. rendszeradminisztrátor,

d. rendszerüzemeltető,

e. független rendszervizsgáló,

f. regisztrációs felelős.

Jelen pont 1. táblázatában a hitelesítés- az Időbélyegzés és az OCSP szolgáltatásokhoz kapcsolódó munkakörök, azok feladat-, felelősség és hatáskörei kerülnek összefoglalásra.

Munkakör	Feladatkör	Felelősségi kör	Hatáskör
A Szolgáltató infokommunikációs divíziójának vezetője	A Szolgáltató szervezet irányítása és ellenőrzése	Folyamatos és biztonságos szolgáltatás. A Szolgáltató informatikai rendszeréért általánosan felelős vezető	A Szolgáltató szervezet szintjén dönt
A PKI Szolgáltató Egység vezetője	A Szolgáltató hitelesítés-szolgáltatási tevékenységének irányítása	Folyamatos és biztonságos szolgáltatás. A PKI Rendszer működtetésének egyszemélyi felelős vezetője	A PKI Szolgáltató Egység szintjén dönt, intézkedik.
Ügyfélkapcsolati Iroda vezetője	Az ügyfélkapcsolati tevékenység irányítása és ellenőrzése.	Az ügyfelek biztonságos azonosítása. Előfizetői szerződések előkészítése	Az ügyfélkapcsolati tevékenység ellenőrzése.
A Szolgáltató IB vezetője (biztonsági tisztségviselő)	IB tevékenység irányítása, ellenőrzése a Szolgáltató minden területén.	A szolgáltatás biztonságáért általánosan felelős személy	IB intézkedések, IB belső ellenőrzés.
Rendszerüzemeltető	Üzemeltetési adminisztráció, hibaelhárítás, karbantartás	A PKI Rendszer folyamatos üzemeltetése, mentése és helyreállítása	Operatív intézkedés az üzemeltetés területén
Rendszeradminisztrátor	Biztonsági beállítások, adminisztráció, karbantartás	A PKI Rendszer telepítése, konfigurálása, karbantartása	Operatív ellenőrzés, operatív intézkedés

Munkakör	Feladatkör	Felelősségi kör	Hatáskör
Hitelesítő biztonsági felügyelő (Security Officer /SO/) (biztonsági felelős)	RO kulcsok, tanúsítványok létrehozása	Szolgáltatói kulcsok, PKI, Időbélyegzés és OCSP alkalmazás és adatok biztonsága	Szolgáltatói (pl.: RO) kulcspárok, tanúsítványok létrehozása
Regisztrációs felügyelő (Registration Officer /RO/) (regisztrációs felelős)	Regisztrációs Iroda irányítása. Előfizető regisztráció, kulcs, tanúsítvány igénylése, kulcs megszemélyesítése	Regisztrációs Iroda folyamatos működtetése.	Regisztrációs Irodán intézkedési jog. SO hatásköre nem lehet.
Rendszervizsgáló (auditor)	Operatív funkcionális és biztonsági ellenőrzések (naplózott, illetve archivált állományok vizsgálata).	Funkcionális és biztonsági hiányosságok, visszaélések felfedése. Kontroll intézkedések betartásának ellenőrzése.	Biztonsági és audit naplók ellenőrzése.

1. táblázat

5.3.2. Az egyes feladatokhoz szükséges személyzeti létszámok

A PKI rendszerben minden rendszer-telepítési, hardver-konfigurálást és szoftver-frissítést igénylő beavatkozást csak két munkatárs egyidejű jelenlétében lehet elvégezni. A műveletek sikerességét auditorok ellenőrizik és hitelesítik.

A Szolgáltató vezetője által kijelölt bizottság jelenlétében végezhetők az alábbi feladatok:

a. Root CRL generálás
b. a szolgáltatói nyilvános kulcsokat tartalmazó token Root CA-hoz való továbbítása, illetve a Root CA által kibocsátott tanúsítványok visszaszállítása
c. a Root CA nyilvános kulcsát tartalmazó tokennek a Produktív CA-hoz való továbbítása
d. időbélyegző egység hitelesítése

Továbbá csak két bizalmi munkakört betöltő személy (SO) együttesen végezheti - fizikailag védett környezetben, más személyek jelenlétét kizárva - az alábbi feladatokat:

a. szolgáltatói magánkulcsok létrehozása
b. a szolgáltatói magánkulcsok biztonsági mentése
c. a szolgáltatói magánkulcsok mentésből történő visszaállítása
d. a szolgáltatói magánkulcsok (és másodpéldányainak) megsemmisítése
e. az RO szolgáltatói kulcspárok generálása, cseréje és megsemmisítése.

5.3.3. A bizalmi munkakörökben elvárt azonosítás és hitelesítés

A bizalmi munkakört betöltő munkatársak PKI alkalmazásokba erős azonosítás-hitelesítési eljárással, pl. szolgáltatói tanúsítvánnyal rendelkező csipkártya kártyaolvasóba helyezésével, majd az azt aktivizáló PIN kód megadásával lépnek be.

5.3.4. Egymást kizáró munkakörök

A bizalmi munkakörök közötti személyi átfedésekre az alábbi korlátozások vonatkoznak:

a. a biztonsági tisztviselő és a regisztrációs felelős nem töltheti be a független rendszervizsgáló munkakört,
b. a rendszeradminisztrátor nem töltheti be a biztonsági tisztviselő és a független rendszervizsgáló munkakört,
c. az informatikai rendszerért általánosan felelős vezető nem töltheti be a biztonsági tisztviselő és a független rendszervizsgáló munkakört,
d. törekedni kell a bizalmi munkakörök teljes személyi elválasztására.

5.3.5. Személyzetre vonatkozó előírások

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

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

A Szolgáltató valamennyi bizalmi munkakört betöltő munkatársa független minden olyan ütköző érdektől, ami hátrányosan érinthetné a hitelesítés-szolgáltató tevékenységeinek semlegességét.

A Szolgáltató munkatársai a feladatok szétválasztása és a legkisebb meghatalmazás szempontjai szerint meghatározott munkaköri leírásokkal rendelkeznek. A munkaleírások meghatározzák a beosztás érzékenységét, a feladatok és a hozzáférési szintek, a háttérellenőrzés, az alkalmazott képzettség és tudatosság alapján. Ahol erre szükség van, megkülönböztetik az általános funkciókat és a hitelesítés-szolgáltató specifikus funkciókat. A munkaköri leírások tartalmazzák a szakismeretre és a tapasztalatra vonatkozó követelményeket is.

5.3.6. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

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

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

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

5.3.7. Biztonsági háttér ellenőrzésekre vonatkozó eljárások

Az alább meghatározott szerepkörök betöltését az átlagosnál magasabb szintű biztonsági ellenőrzés előzi meg:

a. A PKI Szolgáltató Egység vezetője
b. A Szabályozási Csoport vezetője
c. Ügyfélkapcsolati Iroda vezetője
d. A Szolgáltató IB vezetője
e. IB adminisztrátor
f. Hitelesítő biztonsági felügyelő (Security Officer /SO/)
g. Regisztrációs felügyelő (Registration Officer /RO/)
h. rendszer auditor

A munkakörök betöltéséhez szükséges képzettség és gyakorlat:

A Szolgáltató informatikai rendszeréért általánosan felelős vezető kinevezéséhez szakirányú felsőfokú végzettség és legalább három év, az informatikai biztonsággal összefüggésben szerzett gyakorlat szükséges.

biztonsági tisztviselő (IB adminisztrátor, SO):

- szakirányú közép vagy felsőfokú végzettség,
- középfokú végzettség esetén legalább három, felsőfokú végzettség esetén legalább egy év informatika biztonsággal összefüggésben szerzett szakmai gyakorlat,

regisztrációs biztonsági tisztviselő (RO):

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

működtető adminisztrátor, rendszer auditor:

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

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

A szerepkörhöz történő hozzárendeléskor:

a. pontos és írásos munkaköri leírást kell átvennie a fölérendelt vezetőtől,
b. titoktartási nyilatkozatot kell a kijelölt személlyel aláíratni, amelyben 3 év titoktartási kötelezettség szerepel a Szolgáltatótól történő kilépés utáni időponttól számítva,
c. a szükséges mértékű oktatásban kell a kijelölt személyt részesíteni, annak érdekében, hogy a feladat-, felelősség és hatáskörét pontosan megismerje és gyakorolni tudja.

Kilépéskor:

a. A kilépésről szóló döntés meghozatalakor a kilépő fizikai és logikai belépési és hozzáférési jogosultságait azonnal meg kell szüntetni. A kilépő ezután az informatikai biztonsági menedzser kíséretében léphet be még egyszer a munkahelyi környezetébe, a személyes dolgai elvitele céljából.

b. A kilépő személy számítógépes tevékenységét legalább két hétre visszamenőlegesen le kell ellenőrizni.

c. Vissza kell venni az aláírás-létrehozó eszközét, azonnal és dokumentáltan meg kell semmisíteni azt. A kapcsolódó tanúsítvány(oka)t azonnal vissza kell vonni.

d. Minden, a kilépőnél levő dokumentációt és ügyiratot vissza kell venni, különös tekintettel a biztonsági és/vagy minősített adatokat információkat tartalmazó anyagokra.
A visszaadott anyagokról tételes átvételi jegyzőkönyvet kell felvenni.

Nem tölthet be bizalmi munkakört az a személy, akinél a biztonsági ellenőrzés kockázatot tár fel.

5.3.8. Képzési követelmények

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

Rendszerüzemeltetői munkakörbe kinevezett munkatárs a kinevezést követő 3 hónapig, megfelelő gyakorlattal rendelkező kollégával közösen van beosztva.

5.3.9. Továbbképzési gyakoriságok és követelmények

Abban az esetben, amikor a szolgáltatásban jelentős változás[10] következik be, valamennyi munkatárs, az őt érintő mélységben továbbképzésben részesül, illetve megkapja a számára szükséges dokumentációkat.[11]

Kisebb változások[12] bekövetkezése előtt a munkatársak írásos tájékoztatást kapnak a változásokról.

5.3.10. A felhatalmazás nélküli tevékenységek büntető következményei

Valamennyi bizalmi munkakört betöltő munkatárs a munkaköri kinevezéssel:

a. írásos tájékoztatást kap jogszabályi kötelezettségeiről, jogairól, a személyes adatai kezelésére vonatkozó minősítési és kezelési szabályokról

b. munkaköri leírása tartalmazza az őt érintő biztonsági feladatokat

c. titoktartási nyilatkozatot ír alá

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

5.3.11. A szerződéses alkalmazottakra vonatkozó követelmények

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

Az egyéb feladatok ellátására, vállalkozási vagy megbízásos szerződésben foglalkoztatott személyeket a Szolgáltató csak az „ellenőrzött beszállítók" listájáról választ. Az ellenőrzött beszállítókkal a Szolgáltató írásos megállapodást köt, amelyben rögzíti a biztonsági szabályokat.

Valamennyi szerződő fél titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a munkavégzés során birtokába kerülő üzleti titkokat és bizalmas információkat illetéktelen személynek fel nem fedi, s egyéb módon sem hasznosítja. A titoktartási nyilatkozat záró része tartalmazza a megszegése esetén alkalmazandó szankciókat is.

5.3.12. A személyzet számára biztosított dokumentációk

A személyzet számára biztosítandó dokumentációt a 9.1 pont sorolja fel.

---

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

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

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

6.Műszaki biztonsági óvintézkedések

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

A hibák (különösen a telepítési és karbantartási hibák) elkerülése érdekében rendszer-telepítési, hardver-konfigurálást és szoftver-frissítést igénylő beavatkozást csak két munkatárs egyidejű jelenlétében lehet elvégezni. A műveletek sikerességét auditorok ellenőrizik és hitelesítik.

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

A Szolgáltató a szolgáltatás nyújtásához a következő elektronikus aláírási terméket használja:

Nagy biztonságú hardver modul (HSM[13]) IBM 4758-002 PCI (co-processzor)

Tanúsítva: HUNG-T-030-2006

6.1. Kriptográfiai kulcspár előállítás és aláírás-létrehozó eszköz megszemélyesítés

6.1.1. Kulcspár előállítás

A Szolgáltató maga generálja a szolgáltatói kriptográfiai kulcspárokat (az aláírás-létrehozó és az aláírás-ellenőrző adatokat) fizikailag védett környezetben, nagy biztonságú hardver modulban (HSM), kettős ellenőrzés mellett. A nagy biztonságú hardver modul hazai tanúsítvánnyal rendelkezik és szerepel a Nemzeti Hírközlési Hatóság által jóváhagyott minősített elektronikus aláírási termékek listájában. A kulcspárok generálását olyan algoritmussal végzi, melyet jogszabály ismer el erre a célra alkalmasnak.[14]

A Szolgáltató nem fogad el az Előfizető által generált kulcspárt.

Biztonságos aláírás-létrehozó eszköz alkalmazása esetén (MÁV INFORMATIKA Kft. MTT+BALE hitelesítési rend, IHM ajánlása a közigazgatásban alkalmazható hitelesítési rendekre, 1. számú melléklet) a kriptográfiai kulcspárt a Szolgáltató PKI alkalmazása magán a biztonságos aláírás-létrehozó eszközön generálja.

Aláírás-létrehozó eszköz alkalmazása esetén (MÁV INFORMATIKA Kft. MTT hitelesítési rend) a kriptográfiai kulcspárt a Szolgáltató PKI alkalmazása biztonságos környezetben generálja.

A kriptográfiai magánkulcsok (aláírás-létrehozó adatok) teljes életciklusuk alatt a nagy biztonságú hardver modulban, illetve a biztonságos aláírás-létrehozó eszközön maradnak, amennyiben ilyen módon kerültek generálásra.

Az időbélyeget illetve az OCSP választ aláíró szolgáltatói kulcsot az időbélyegző egység szerves részét képező, tanúsított HSM modul generálja és tárolja. Az aláíró kulcs teljes életciklusa alatt ezen eszközben marad.

6.1.2. Az aláírás-létrehozó eszköz megszemélyesítése

A biztonságos aláírás-létrehozó eszköz (chip kártya) megszemélyesítését a Szolgáltató maga végzi fizikailag védett környezetben üzemelő kártya-megszemélyesítő rendszeren.

A chip kártya megszemélyesítés szolgáltatáshoz vizuális megjelenítés, egy oldali nyomással történő grafikus megszemélyesítés is kapcsolódik az Előfizetői Szerződésben meghatározott adattartalommal.

A Szolgáltató az aláírás-létrehozó adat aktivizálásához (a chip kártyához) PIN kódot biztosít. A PIN kódot fizikailag védett környezetben állítja elő és a kódot tartalmazó PIN-borítékot az aláírás-létrehozó eszköztől elkülönítve tárolja.

6.1.3. Az aláírás-létrehozó adat eljuttatása az Aláíróhoz (Előfizetőhöz)

A Szolgáltató az aláírás-létrehozó adatot, illetve a megszemélyesített biztonságos aláírás-létrehozó eszközt az átvételig fizikailag védett környezetben tárolja és biztosítja, hogy az aláírás-létrehozó adat titkossága ne sérüljön.

A Szolgáltató az aláírás-létrehozó eszközt és a PIN kódot tartalmazó borítékot személyesen adja át az Aláírónak (Előfizetőnek).

Az aláírás-létrehozó eszköz és a PIN kód átvételét követően csak az Aláíró férhet hozzá saját magánkulcsához.

Az aláírás-létrehozó eszköz átvételének megtagadása visszavonási kérelemnek számít.

---

[13] HSM: Hardware Security Module

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

6.1.4. Az Aláírók aláírás-ellenőrző adatának eljuttatása az érintett feklekhez

A Szolgáltató az Aláírók aláírás-ellenőrző adatát (nyilvános kulcsát) Tanúsítványtárában teszi mindenki számára elérhetővé. Az Aláírók aláírás-ellenőrző adata az Előfizetői tanúsítványba van foglalva.

6.1.5. A Szolgáltató aláírás-ellenőrző adatainak eljuttatása a felhasználói közösséghez

A Tanúsítványtárban közzétett tanúsítványok ellenőrzéséhez szükséges szolgáltatói nyilvános kulcsok (szolgáltatói tanúsítványok) és visszavonási listák a Szolgáltató Internetes honlapján keresztül közvetlenül elérhetők.

A tanúsítványok letölthetők és a felhasználók kliens-alkalmazásaiba installálhatók.

6.1.6. Kulcs méretek, algoritmosok

A Szolgáltató hitelesítő központjai elektronikus aláírás létrehozására az RSA[15] algoritmust használják.

A Hitelesítő Központok ("Root CA", „Produktív CA") aláíró kulcsainak mérete:	2048 bit
Az időbélyegző egység aláíró kulcsának mérete:	2048 bit
Az Aláírók aláíró kulcsainak (aláírás-létrehozó adatának) mérete:	legalább 1024 bit

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

6.1.7. Előfizetői aláírás-ellenőrző adat előállításához használt paraméterek előállítása

Az előfizetői tanúsítványok az RSA aláíró algoritmusokhoz használhatók.

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

6.1.8. Szolgáltatói kulcsgenerálás

A szolgáltatói tanúsítványokhoz a kulcsgenerálás nagy biztonságú hardver modulban (HSM-ben) vagy biztonságos aláírás-létrehozó eszközön történik.

A produktív hitelesítő központok és az időbélyeget aláíró kulcsok tanúsítványait a Szolgáltató 1. szintű hitelesítő központja (Root CA-ja) hitelesíti.

6.1.9. Kulcs felhasználási célok

A Szolgáltató Előfizetők részére tanúsítványt (kulcspárt) kizárólag elektronikus aláírási célra bocsát ki.

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

Nem a Ket hatálya alá tartozó Előfizetők részére kibocsátott tanúsítványok bővítmény (Extension) részében található „KeyUsage" mezőbe elektronikus aláírás felhasználási célként – az NR mellett - a „DigitalSignature" (DS) kulcshasználat is szerepeltethető.

6.2. Aláírás-létrehozó adat védelme

6.2.1. A HSM-re vonatkozó szabványok

Az Előfizetők aláírás-létrehozó adatának előállítására a Szolgáltató olyan eszközt használ, amely teljesíti a CC EAL4 követelményeket, rendelkezik hazai tanúsítással és szerepel a NHH által regisztrált BALE eszközök listájában.

A Szolgáltató saját szolgáltatói magánkulcsainak tárolására illetve használatára olyan biztonságos kriptográfiai modult (HSM) alkalmaz, amely teljesíti a vonatkozó (Eat. 7. § (5)-(6) bekezdéseiben foglalt) feltételeket, azaz rendelkezik az NHH által regisztrált, illetve az Európai Unió valamely tagállamában nyilvántartásba vett tanúsításra jogosult szervezetek által kiadott igazolással.

[15] 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.

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

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

6.2.3. Aláírás-létrehozó adat letét

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

6.2.4. Aláírás-létrehozó adat mentése, duplikálása

A Szolgáltató az Előfizető aláírás-létrehozó adatot semmilyen formában nem menti vagy tárolja.

A Szolgáltatónál a Hitelesítő Központ aláíró magánkulcsai[16] biztonsági okokból duplikálásra kerülnek. A mentés titkosított formában, speciális eszközök alkalmazásával történik.

6.2.5. Aláírás-létrehozó adat kriptográfiai modulba helyezése

HSM modulban generált szolgáltatói kulcspárok esetében a magánkulcs nyílt (titkosítatlan) formában semmilyen körülmények között sem hagyhatja el a modult.

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

A Szolgáltató munkatársai számára a PKI biztonsági felügyelő (SO) generálja a kulcspárokat a biztonságos aláírás-létrehozó eszközön, és a magánkulcsok semmilyen körülmények között nem hagyják el azokat.

Az előfizetői kulcspárokat a szolgáltató kizárólag a biztonságos aláírás-létrehozó eszközön generálja, így a magánkulcsok semmilyen körülmények között nem hagyják el azokat. A biztonságos aláírás-létrehozó eszközt a Szolgáltató PIN-kóddal védve adja át az Előfizetőnek.

6.2.6. Aláírás-létrehozó adat aktiválása

Az előfizetői aláírás-létrehozó adat aktiválása az Aláíró által történik a PIN kód megadásával. Biztonságos aláírás-létrehozó eszköz használata esetén az aláírás-létrehozó adat az aktiváláskor sem hagyja el a csipkártyát, azt onnan leolvasni nem lehet.

6.2.7. Aláírás-létrehozó adat deaktiválása

Az előfizetői aláírás-létrehozó adatok deaktiválását az Aláíró alkalmazása végzi kijelentkezéskor vagy – BALE használata esetén – amikor az Aláíró a csipkártyát eltávolítja az olvasóból.

6.2.8. Aláírás-létrehozó adat megsemmisítése

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

A szolgáltatói aláírás-létrehozó adatok megsemmisítése a Szolgáltató kötelessége.

6.3. Kulcspár kezelés egyéb aspektusai

6.3.1. Aláírás-ellenőrző adat archiválása

Az aláírás-ellenőrző adatokat a tanúsítványok tartalmazzák. A Szolgáltató minden általa előállított és kibocsátott tanúsítványt archivál az érvényesség lejártától számított 10 évig.

Az archiválás biztonsági okokból 2 példányban történik.

6.3.2. Aláírás-létrehozó és aláírás-ellenőrző adatok felhasználási ideje

Az aláírás-létrehozó adat (aláíró kulcs) és az aláírás-ellenőrző adat (nyilvános kulcs) érvényességi ideje megegyezik a kulcsok hitelességét igazoló tanúsítvány érvényességi idejével:

Root CA aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 20 év
Időbélyegző egység aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 10 év

[16] A kriptográfiai hardver modul (tanúsítványokat, illetve visszavonási listákat aláíró) magánkulcsai.

OCSP válasz egység aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 10 év
Produktív CA aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 20 év
RO kommunikációs kulcs és tanúsítvány érvényessége:	legfeljebb 3 év
Előfizetői aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 1 év
Előfizetői tanúsítvány leghosszabb érvényességi ideje:	legfeljebb 2 év

A tanúsítványok és a benne foglalt aláírás-ellenőrző adatok (nyilvános kulcsok) érvényességének kezdete a kibocsátás időpontjával (év, hónap, nap, óra, perc, másodperc) egyezik meg.

6.4. Aktiválási adatok

6.4.1. Aktiválási adatok generálása és installációja

Az aláírás-létrehozó eszközök aktivizáló adatait (PIN kódjait) a PKI alkalmazás állítja elő.

6.4.2. Aktiválási adatok védelme

A Szolgáltató az Aláíró hozzáférési jogosultságát ellenőrző adatot (PIN-kódot) csak abból a célból rögzítheti, hogy azt az Aláíró számára - másolat megőrzése nélkül - átadhassa[17].

A Szolgáltató az aláírás-létrehozó eszközök PIN kódjait műszaki és szervezési intézkedésekkel védi az Előfizetőnek vagy az Aláírónak történő átadásig.

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

Az Előfizető a későbbiekben is bármikor megváltoztathatja a PIN kódját.

Előfizetői aláírás-létrehozó adatának kizárólag csak az Aláíró által történő birtoklása az alapvető feltétel az elektronikusan aláírt adat, dokumentum hitelességének biztosítására. Emiatt az Előfizetőnek saját felelősségi körében kell biztosítania az aktivizáló adat kizárólagos birtoklását. Amennyiben ez sérül vagy elveszik, illetve ennek alapos gyanúja fennáll, akkor az Előfizetőnek ezt haladéktalanul jelentenie kell az Ügyfélkapcsolati Irodánál vagy az Ügyfélszolgálatnál, amely azonnal intézkedik a tanúsítvány visszavonásáról.

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

A Szolgáltató a saját aktiválási adatait a MeH ITB 12. ajánlás által meghatározott fokozott biztonsági szinten védi.

6.4.3. Aktiválási adatok egyéb aspektusai

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

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

6.5. Az időszinkronizálás megvalósítása

A Szolgáltató által adott időbélyeg felépítése megfelel az RFC 3161 szabványnak és a Szolgáltató [11] Időbélyegzési rendjében (ISZR) meghatározott további követelményeknek.

Az időszinkronizáció menetét a Szolgáltató [11] Időbélyegzési Rendje 7.3. pontja írja le.

A Szolgáltató által alkalmazott referencia időforrások:

server 148.6.0.1	ubul.kfki.hu
server 129.132.2.21	swisstime.ee.ethz.ch
server 192.53.103.103	ptbtime1.ptb.de
server 145.238.110.49	ntp-p1.obspm.fr
server 192.168.6.90	gps time

A referencia időforrások pontossága századmásodpercen belül van.

[17] 3/2005. (III. 18.) IHM rendelet 40. §, 4. bek. szerint.

6.6. Számítógép biztonsági szabályok

6.6.1. Számítógép biztonság technikai követelményei

A Számítógép biztonság technikai követelményeit a MeH ITB 12. ajánlás szerinti fokozott biztonsági osztálybasorolás határozza meg.

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

a. operációs rendszer,
b. PKI alkalmazás, időbélyegzés és OCSP alkalmazás,
c. kriptográfiai hardver modulok,
d. tűzfalak, behatolás detektorok.

Az operációs rendszerek által megvalósított biztonsági funkciók az alábbiak:

a. biztonsági naplózás (a biztonsági napló védelme, az ahhoz való hozzáférés korlátozása),
b. a felhasználói adatok védelme (a felhasználói adatok csak alkalmazáson keresztüli elérésének biztosítása),
c. azonosítás és hitelesítés (a hozzáférési jogosultságok szerepkörök szerinti beállítása, módosítása),
d. a biztonsági funkciók védelme (a hozzáférés ellenőrzés megkerülhetetlenségének biztosítása).

A PKI alkalmazás által megvalósított biztonsági funkciók az alábbiak:

a. biztonsági naplózás (a rendszerüzemeltetői hozzáférések és tevékenységek rögzítése),
b. kommunikáció (a Hitelesítő Központ és a Regisztrációs Iroda közötti kommunikáció bizalmasságának, sértetlenségének és hitelességének biztosítása),
c. a felhasználói adatok védelme (az elindított alkalmazások csak a jogosultságnak megfelelő funkciók elérhetőségét biztosítják),
d. azonosítás és hitelesítés (a rendszerüzemeltetők azonosítása, hitelesítése, az alkalmazások által biztosított funkciók elérésének sikeres hitelesítéshez kötése).

Az időbélyegzésre és OCSP szolgáltatásra vonatkozó biztonsági funkciók az alábbiak:

a. Az időbélyeget ileltve OCSP választ aláíró kulcsok tárolása a tanúsítással rendelkező HSM egység(ek)ben történik. Az időbélyegző illetve OCSP szerverek külön biztonsági zónában történő üzemeltetése.
b. Az időbélyegző és OCSP szerverek belső órájának pontossága folyamatos ellenőrzés alatt áll. A pontossági tartományból történő kilépés esetén az időbélyegző illetve OCSP szolgáltatás leáll és a hiba kijavításáig minden további kérésre hibaüzenet kerül kiküldésre.
c. A szinkronizáló órajelek hitelességét az időbélyegző illetve OCSP informatikai rendszer indításakor egy erre a célra létrehozott bizottság tanúsította.
d. biztonsági naplózás,
e. Az időbélyeget illetve OCSP választ kibocsátó szervereket többszörös tűzfal rendszer védi a külső hálózatokról érkező fenyegetésektől.
f. Az időbélyegzés és OCSP szolgáltatás rendelkezésre állási szintje 99,9%. Ez a szint meleg tartalékolt időbélyegző illetve OCSP szerver architektúrával, és a szervereknek a hitelesítés szolgáltató informatikai rendszer magas rendelkezésre állást felügyelő és vezérlő rendszerébe történő integrálásával biztosított

A kriptográfiai hardver modulok által megvalósított biztonsági funkciók az alábbiak:

a. biztonsági naplózás,
b. kriptográfiai támogatás (kriptográfiai kulcsok generálása, védelme és megsemmisítése; bizalmasságot, sértetlenséget, hitelességet és letagadhatatlanságot biztosító kriptográfiai eljárások megvalósítása),
c. a felhasználói adatok védelme (hozzáférés ellenőrzési szabályok érvényre juttatása),
d. azonosítás és hitelesítés,
e. biztonságkezelés (a hozzáférési jogosultságok szerepkörök szerinti beállítása, módosítása),
f. a biztonsági funkciók megbízható védelme (a hozzáférés ellenőrzés megkerülhetetlenségének biztosítása),
g. megbízható út/csatorna (megbízható útvonal kiépítése a magát hitelesítő felhasználóval, mely alkalmas az átvitt adatok illetéktelen felfedésének és módosításának megakadályozására).

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

a. biztonsági naplózás (a hálózati kommunikáció naplózása, a biztonsági napló védelme, a napló folyamatos elemzése: biztonsági riasztások és automatikus válaszok megvalósítása),

b. a felhasználói adatok védelme (az információ áramlás ellenőrzési szabályok érvényre juttatása/szűrés, a tiltott információ áramlás megakadályozása, megfigyelése),

c. azonosítás és hitelesítés,

d. a biztonsági funkciók megbízható védelme (az információ áramlás ellenőrzés megkerülhetetlenségének biztosítása),

6.6.2. Számítógép biztonsági értékelések

A számítógép biztonsági értékelések rendszerét a 2. táblázat mutatja.

Biztonsági ellenőrzés típusa		Végzi	Rendszeresség
Operatív	IT infrastruktúra	Informatikai biztonsági adminisztrátor	Naponta
	PKI alkalmazás	Rendszer auditor	Naponta
Belső ellenőrzés	IT infrastruktúra	Informatikai biztonsági menedzser	Félévente egyszer
	PKI alkalmazás	Hitelesítési Rend és Szabályozási Csoport	Félévente egyszer
Külső ellenőrzés	IT infrastruktúra	Külső auditor	Évente egyszer
	PKI alkalmazás	Külső auditor	Évente egyszer

2. táblázat

6.7. Életciklus technikai szabályok

6.7.1. Rendszerfejlesztési szabályok

Az IT életciklusra vonatkozó rendszerfejlesztési szabályokat a Szolgáltató társasági szintű informatikai biztonságpolitikája és informatikai biztonsági szabályzat tartalmazza, amelyek pontosan meghatározzák az előkészítés, a projekt, a működtetés, a menedzselés és a visszavonás/rekonstrukció ciklus időszakok feladatait és az alkalmazott módszertanokat.

6.7.2. Biztonságkezelési szabályok

A biztonságkezelési szabályokat a Szolgáltató társasági szintű informatikai biztonságpolitikája, a társasági és a rendszer szintű informatikai biztonsági szabályzatok tartalmazzák.

6.7.3. Életciklus biztonsági értékelések

A Szolgáltató által alkalmazott megbízható informatikai rendszerek a MeH ITB 12. ajánlás fokozott biztonsági osztálya követelményeinek felelnek meg, amely azonos szintű az ITSEC F-B1/E3, illetve a Common Criteria EAL4 szintnek. Az életciklus biztonsági értékelések a 2. táblázat szerinti rendszerben történnek.

6.8. Hálózati biztonsági szabályok

A hálózati védelmi intézkedések a MeH ITB 12. ajánlás fokozott biztonsági osztálya biztonsági szintnek felelnek meg.

A Hitelesítő Központ és a Regisztrációs Iroda közötti kommunikációt biztosító belső hálózat PKIX kapcsolattal védett a sértetlenség és letagadhatatlanság érdekében, illetve bizalmasság elvesztése ellen.

A Szolgáltató hitelesítés-szolgáltatást, időbélyegzést és OCSP-t támogató informatikai rendszerénél a védett belső és a külső hálózatok biztonságos elválasztását tűzfal és behatolás érzékelő rendszer (IDS) biztosítja.

A Hitelesítő Központ nem folytat közvetlen külső kommunikációt a végfelhasználókkal.

6.9. Kriptográfiai (HSM) modul ellenőrzése

A kriptográfiai modulok ellenőrzik az illetéktelen beavatkozási kísérleteket. Ha egy modul ilyet detektál, akkor:

a. a memóriájában levő magánkulcsot törli

b. a modul saját tanúsítványa is törlésre kerül és ezzel a modul használhatatlanná válik

7. Tanúsítvány és tanúsítvány-visszavonási profil

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

7.1. Tanúsítvány profil

7.1.1. Alap mezők

A Szolgáltató az RFC 2459-nek megfelelő tanúsítványokat bocsát ki.

7.1.2. Tanúsítvány kiterjesztések

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

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

7.1.3. Ket. hatálya alá tartozó tanúsítványok

A Ket. hatálya alá tartozó tanúsítványok megfelelnek "Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára" előírásainak.

7.2. Tanúsítvány-visszavonási profil

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

Szolgáltató a kiterjesztéseket nem köteles kitölteni.

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

7.3. Időbélyeg profil

A Szolgáltató által kibocsátott időbélyegek szerkezete követi az RFC 3161 szabványt és az ETSI ET 102 023 szabvány 7.3.1 pontjában előírtakat.

7.4. OCSP profil

A Szolgáltató által befogadott OCSP kérések és a kibocsátott OCSP válaszok szerkezete követi az RFC 2560 szabványt.

8.HSZSZ-M adminisztráció

8.1. HSZSZ-M változatkezelési eljárások

8.1.1. HSZSZ-M változtatási eljárások

A Szolgáltató szervezetén belül Hitelesítési Rend és Szabályozási Csoport működik, amely felelős a jelen HSZSZ-M karbantartásáért. A változtatási igényeket e csoport fogadja és gyűjti össze, elvégzi a módosításokat, eleget tesz a belső és külső tájékoztatási kötelezettségeknek, s életbe lépteti a változtatásokat.

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

A HSZSZ-M módosított változatai mindig új verziószámmal kerülnek nyilvánosságra.

8.1.2. Értesítéssel változtatható elemek

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

8.1.3. Szabályzati objektumazonosítót változtató módosítások

Minden olyan jelentősebb módosítás, melyet a Szolgáltató csak az újonnan kibocsátásra kerülő tanúsítványok esetében alkalmaz (s a már kibocsátottak esetében nem) a HSZSZ-M verziószámának fő számjegyét, s a szabályzat objektumazonosítóját (OID) is módosítja.

8.2. Közzétételi és tájékoztatási elvek

8.2.1. A HSZSZ-M-ben nem tárgyalt elemek

A Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatások biztonságát nem veszélyezteti. A Szolgáltató több belső biztonsági és egyéb szabályzattal, operatív szintű előírással rendelkezik, melyeket bizalmasan kezel (lásd: 9.1 fejezet). A 2.7 pontban leírt tanúsítási eljárások ezeket a dokumentumokat is vizsgálják.

8.2.2. A HSZSZ-M közzététele

A Szolgáltató a jelen szabályzatát Internetes honlapján teszi közzé.

8.3. HSZSZ-M elfogadási eljárások

A jelen HSZSZ-M megfelel az RFC 2527 szabványnak. A megfelelőségi vizsgálatot a Szolgáltató, illetve a külső auditor is elvégzi a 2. táblázatban megadott rendszerességgel.

A szabályzat törvényeknek való megfelelőségét a Nemzeti Hírközlési Hatóság is vizsgálja a HSZSZ-M aktuális változatának hatálybalépését megelőzően.

Módosítás esetén a Szolgáltató a HSZSZ-M változtatásokkal egybeszerkesztett új verziójának tervezetét hatósági felülvizsgálat és nyilvántartásba vétel céljából átadja a Nemzeti Hírközlési Hatóságnak. A Szolgáltató alkalmanként ezt megelőzően is konzultál a Nemzeti Hírközlési Hatósággal a tervezett változtatásairól. A HSZSZ-M új változat hatályba léptetésének feltétele, hogy azt a Nemzeti Hírközlési Hatóság nyilvántartásba vette.

9.Hivatkozások és Meghatározások

9.1. Hivatkozások

A hivatkozott jogszabályokat, ajánlásokat és szabványokat az 1.2.2 fejezet tartalmazza.

Az Informatikai és Hírközlési Minisztérium elfogadott ajánlásai, szabályzatai:

[1] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható hitelesítési rendekre (2005. december 7.)

[2] Közigazgatási, ügyfélhez kapcsolódó, biztonságos aláírás-létrehozó eszköz használatát megkövetelő, aláírás célú tanúsítványokhoz tartozó, minősített hitelesítési rend /Azonosító: [MHR_Ü], OID: 0.2.216.1.100.42.101.1.2.1/

[3] Közigazgatási, köztisztviselőhöz kapcsolódó, biztonságos aláírás-létrehozó eszköz használatát megkövetelő, aláírás célú tanúsítványokhoz tartozó, minősített hitelesítési rend /Azonosító: [MHR_K], OID: 0.2.216.1.100.42.101.2.2.1/

A Szolgáltató hivatkozott szabályzatai:

[4] A MÁV INFORMATIKA Kft. Szervezeti és Működési Szabályzata,

[5] A MÁV INFORMATIKA Kft. Iratkezelési Szabályzata

[6] A MÁV INFORMATIKA Kft. Titokvédelmi Szabályzata

[7] A MÁV INFORMATIKA Kft. Informatikai Biztonságpolitikája

[8] A MÁV INFORMATIKA Kft. Informatikai Biztonsági Szabályzata

[9] Hitelesítési Rend nyilvános körben kibocsátott biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített tanúsítványokra (HR-MTT+BALE)

[10] Hitelesítési Rend nyilvános körben kibocsátott minősített tanúsítványokra (HR-MTT+BALE)

[11] Időbélyegzési Szolgáltatási Rend (ISZR)

[12] Általános Szerződési Feltételek a minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz (ÁSZF-M)

[13] A PKI Szolgáltatások Biztonsági Szabályzata

[14] A PKI Szolgáltatások Üzletmenet-folytonossági Terve

[15] A PK Szolgáltatások Üzemeltetési Kézikönyve

9.2. Meghatározások

Alany: A hitelesítés-szolgáltató által kiadott tanúsítványban azonosított természetes személy, aki a tanúsítványban szereplő nyilvános kulcsnak megfelelő magánkulcsot birtokolja.

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

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

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

Aláíró: az a természetes személy, aki az aláírás-létrehozó eszközt birtokolja és a saját vagy más személy nevében aláírásra jogosult

Biztonságos aláírás-létrehozó eszköz: az Eat. 1. számú mellékletében foglalt követelményeknek eleget tevő, az Eat. 7. § (5) – (6) bekezdés szerinti tanúsítással rendelkező aláírás-létrehozó eszköz

Biztonsági tisztviselő, biztonsági menedzser: a hitelesítés-szolgáltatás biztonságáért, a biztonsági irányelvek és szabályzatok érvényre juttatásáért általánosan felelős személy

Elektronikus aláírás: elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat

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

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

Elektronikus aláírás hitelesítés-szolgáltató: az Eat. 6. § (2) bekezdése szerinti tevékenységet végző személy (szervezet)

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

Elektronikus aláírás érvényesítése: annak tanúsítása minősített elektronikus aláírás vagy e szolgáltatás tekintetében minősített szolgáltató által kibocsátott időbélyegző elhelyezésével, hogy az elektronikus dokumentumon elhelyezett elektronikus aláírás vagy időbélyegző, illetve az azokhoz kapcsolódó tanúsítvány az időbélyegző elhelyezésének időpontjában érvényes volt

Elektronikus aláírási termék: olyan szoftver vagy hardver, illetve más elektronikus aláírás alkalmazáshoz kapcsolódó összetevő, amely elektronikus aláírással kapcsolatos szolgáltatások nyújtásához, így különösen elektronikus aláírások, illetőleg időbélyegző készítéséhez vagy ellenőrzéséhez használható

Elektronikus dokumentum: elektronikus eszköz útján értelmezhető adategyüttes

Érintett fél: Az Érintett fél (aláírás Ellenőrző) olyan természetes vagy jogi személy, aki vagy amely, az aláírt és/vagy időbélyegzett és/vagy OCSP válasszal ellátott elektronikus dokumentum fogadója, és egy adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el az aláírás, és/vagy az időbélyeg és/vagy az OCSP válasz hitelességének ellenőrzésekor.

Érvényességi lánc: az elektronikus dokumentum vagy annak lenyomata, és azon egymáshoz rendelhető információk sorozata, (így különösen azon tanúsítványok, a tanúsítványokkal kapcsolatos információk, az aláírás-ellenőrző adatok, a tanúsítvány aktuális állapotára, visszavonására vonatkozó információk, valamint a tanúsítványt kibocsátó szolgáltató elektronikus aláírás-ellenőrző adatára és annak visszavonására vonatkozó információk), amely alapján megállapítható, hogy az elektonikus dokumentumon elhelyezett fokozott biztonságú vagy minősített aláírás, illetve időbélyegző, valamint az azokhoz kapcsolódó tanúsítványok az aláírás és időbélyegző elhelyezésének időpontjában érvényes volt

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

a. alkalmas az aláíró azonosítására,

b. egyedülállóan az aláíróhoz köthető,

c. olyan eszközökkel hozták létre, amelyek kizárólag az aláíró befolyása alatt állnak és

d. a dokumentum tartalmához olyan módon kapcsolódik, hogy minden - az aláírás elhelyezését követően a dokumentumon tett - módosítás érzékelhető

Hitelesítési rend: olyan szabálygyűjtemény, mely egy tanúsítvány felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára.

Időbélyegzés: az a folyamat, melynek során az elektronikus dokumentumhoz olyan igazolás rendelődik, amely tartalmazza a bélyegzés hiteles időpontját, és amely a dokumentumhoz oly módon kapcsolódik, hogy minden – az igazolás kiadását követő – módosítás érzékelhető

Időbélyeg: elektronikus dokumentumhoz végérvényesen hozzárendelt, vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikus dokumentum az időbélyegzés időpontjában változatlan formában létezett

Időbélyegzés szolgáltatási rend: olyan szabálygyűjtemény, amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) valamely időbélyegző felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára

Igénybe vevő: elektronikus aláírással kapcsolatos szolgáltatást igénybe vevő természetes személy, jogi személy vagy jogi személyiség nélküli szervezet

Igénylő: a minősített tanúsítvány iránti igényt benyújtó személy

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

Kriptográfiai kulcs: olyan kriptográfiai transzformációt vezérlő egyedi jelsorozat, amelynek ismerete a titkosításhoz (rejtjelezéshez) vagy annak visszaállításához, továbbá az elektronikus aláírás előállításához vagy az elektronikus aláírás hitelességének ellenőrzéséhez szükséges

Lenyomat: olyan meghatározott hosszúságú, az elektronikus dokumentumhoz rendelt bitsorozat, amelynek képzése során a használt eljárás (lenyomatképző eljárás) a képzés időpontjában teljesíti a következő feltételeket:

a) a képzett lenyomat egyértelműen származtatható az adott elektronikus dokumentumból;

b) a képzett lenyomatból az elvárható biztonsági szinten belül nem lehetséges az elektronikus dokumentum tartalmának meghatározása vagy a tartalomra történő következtetés;

c) a képzett lenyomat alapján az elvárható biztonsági szinten belül nem lehetséges olyan elektronikus dokumentum utólagos létrehozatala, amelyre alkalmazva a lenyomatképző eljárás eredményeképp az adott lenyomat keletkezik

Minősített elektronikus aláírás: olyan - fokozott biztonságú – elektronikus aláírás, amelyet az aláíró biztonságos aláírás-létrehozó eszközzel hozott létre, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki

Minősített hitelesítés-szolgáltató: az Eat. szabályai szerint nyilvántartásba vett, minősített tanúsítványt a nyilvánosság számára kibocsátó hitelesítés szolgáltató

Minősített szolgáltató: a minősített hitelesítés-szolgáltató és az Eat. 6. § (1) bekezdésének *b)-d)* pontjában meghatározott szolgáltatásokat nyújtó olyan szolgáltató, amely a szolgáltatók nyilvántartásában valamely szolgáltatás tekintetében minősített szolgáltatóként szerepel

Minősített tanúsítvány: az Eat. 2. számú mellékletében foglalt követelményeknek megfelelő olyan tanúsítvány, amelyet minősített szolgáltató bocsátott ki

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

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

Rendszervizsgáló: hitelesítés-szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a hitelesítés-szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy

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

Szolgáltatási szabályzat: az Eat. 6. § (1) bekezdése szerinti szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat

Szolgáltató: elektronikus aláírással kapcsolatos szolgáltatást nyújtó természetes személy, jogi személy vagy jogi személyiség nélküli szervezet

Szolgáltatói kulcspár: a szolgáltatói magánkulcs és a szolgáltatói nyilvános kulcs

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

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

Tanúsítvány: hitelesítés-szolgáltató által kibocsátott digitális igazolás, amely a belefoglalt nyilvános kulcsot (aláírásellenőrző adatot) az Eat. 9. § (3), illetőleg (4) bekezdése szerint egy meghatározott személyhez kapcsolja, és igazolja e személy személyazonosságát.

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

Visszavonás kezelése: az Eat. 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