MÁV INFORMATIKA

Kereskedelmi, Szolgáltató és Tanácsadó Korlátolt Felelosségu Társaság

Szolgáltatási Szabályzat a Minosített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz (HSZSZ-M)

Verziószám	**3.0**
OID szám	**1.3.6.1.4.1.14868.1.2.3**
Hatósági nyilvántartásba vétel napja	**2005. július 22.**
Hatósági nyilvántartásba vétel száma	**HL-12638-4/2005**
Hatálybalépés dátuma	**2005. július 22.**

© Copyright MÁV INFORMATIKA Kft. – Minden jog fenntartva

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

HSZSZ-M verziók

Verzió	Dátum	A változás leírása	Készítette
1.0	2002.09.30	A fokozott biztonságú szolgáltatói regisztrálásra elokészített, a HIF részére átadott változat.	Bodlaki Ákos
2.0	2002.11.29	HSZSZ-M minosített tanúsítványtípusokra, véleményezésre átadott változat	Bodlaki Ákos
2.1	2003.03.31.	A minosítési eljárásra átadott változat kiegészítve és módosítva a HIF észrevételeivel	Bodlaki Ákos
2.2	2003.07.30	Idobélyegzés szolgáltatás minosítési eljárására beadott 1.0 változattal kapcsolatos észrevételekkel módosítva.	Bodlaki Ákos
2.2.1	2004. 01. 20.	Formai és sajtóhibák javítása, belso ellentmondások megszuntetése s zakértoi 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-vel bovített változat	Néder Ferenc

TARTALOMJEGYZÉK

1. Bevezetés — *8*
1.1. Szolgáltató adatai — **8**
1.2. Alapok — **9**
1.2.1. Szabályzat célja — 9
1.2.2. Jogszabályok, szabványok — 9
1.3. HSZSZ-M azonosítás — **10**
1.4. Hitelesítés szolgáltató és felhasználói közösség, alkalmazhatóság — **10**
1.4.1. A Szolgáltató regisztráló és hitelesíto egységei — 11
1.4.2. Elofizetok és Aláírók (Felhasználók) — 11
1.4.3. Érintett felek — 11
1.4.4. Alkalmazhatóság — 11
1.5. Tanúsítvány osztályok, tanúsítványtípusok és tanúsítvány fajták — **12**
1.5.1. Minosített tanúsítványok jellemzoi és típusai — 13
1.5.2. Tanúsítványok használati osztályainak jellemzoi — 14
1.5.3. Tanúsítvány fajták és tulajdonságaik — 14
2. Általános rendelkezések — *15*
2.1. Feladatok és hatáskörök — **15**
2.1.1. A Szolgáltató feladatai és hatásköre — 15
2.1.2. Az Elofizeto és az Aláíró feladatai és hatásköre — 18
2.1.3. Érintett fél feladatai és hatásköre — 18
2.2. Felelosségek — **19**
2.2.1. A Szolgáltató felelossége — 19
2.2.2. Az Elofizeto és az Aláíró felelossége — 20
2.2.3. Érintett fél felelossége — 20
2.3. Az anyagi felelosség mértéke — **20**
2.4. Értelmezés és alkalmazás — **20**
2.4.1. Irányadó jog — 20
2.4.2. Érvénytelenség, hatályosság, megszunés, értesítések — 21
2.4.3. Vitás kérdések kezelése — 21
2.5. Díjak — **21**
2.5.1. Tanúsítvány kibocsátás — 22
2.5.2. Tanúsítvány hozzáférés — 22
2.5.3. Visszavonási lista hozzáférés — 22
2.5.4. Idobélyegzés — 22
2.5.5. OCSP szolgáltatás — 22
2.5.6. Egyéb szolgáltatásokra vonatkozó díjak — 22
2.5.7. Visszatérítési elvek — 22
2.6. Közzététel — **22**
2.6.1. Szolgáltatói információk közzététele — 22
2.6.2. A közzététel gyakorisága — 23

2.6.3. Elérési szabályok 23
2.6.4. Tanúsítványtár 23
2.7. A megfeleloség vizsgálata 23
2.7.1. Vizsgálatok gyakorisága 24
2.7.2. Az átvizsgáló szervezet megnevezése/jellemzoi 24
2.7.3. Hiányosságok kezelése 24
2.7.4. Eredmény kommunikációja 24
2.8. Bizalmasság – Adatkezelési szabályzat 24
2.8.1. Bizalmas információk 24
2.8.2. Nem bizalmas információk 25
2.8.3. Tanúsítvány visszavonási és felfüggesztési okok felfedése 25
2.8.4. Feltárás törvényi meghatalmazással rendelkezok részére 25
2.8.5. Információszolgáltatás polgári eljárás keretében 25
2.8.6. Feltárás tulajdonos kérésére 25
2.8.7. Feltárás más esetekben 25
2.9. Szellemi tulajdonhoz fuzodo jogok 25
3. Azonosítás és hitelesítés 27
3.1. Regisztráció 27
3.1.1. Nevek típusa 27
3.1.2. Nevek szemantikája 27
3.1.3. Nevek egyedisége 27
3.1.4. Név igénylési viták feloldása 27
3.1.5. Védjegyek elismerésének és hitelesítésének módszere 27
3.1.6. Az aláírás-létrehozó adat birtoklás ellenorzésének módszere 27
3.1.7. Személyes azonosság hitelesítése „Személyes” tanúsítvány igénylése esetén 28
3.1.8. Szervezeti identitás hitelesítése „Szervezeti személy” tanúsítvány igénylése esetén 28
3.1.9. Személyi és szervezeti identitás hitelesítése idobélyegzés illetve OCSP szolgáltatás igénylés esetén 29
3.2. Érvényes tanúsítvány megújítása (tanúsítvány frissítése) 30
3.3. Érvénytelen tanúsítvány megújítása 30
3.4. Felfüggesztés és visszavonás kérés 30
4. A muködésre vonatkozó követelmények 31
4.1. Tanúsítványigénylés 31
4.2. Tanúsítvány kibocsátás 31
4.3. Idobélyegzés 31
4.4. OCSP szolgáltatás 32
4.5. Tanúsítvány elfogadás 32
4.6. Tanúsítvány felfüggesztés és visszavonás 32
4.6.1. Visszavonáshoz/felfüggesztéshez vezeto körülmények 32
4.6.2. Visszavonás/felfüggesztés kérelmezése 33
4.6.3. Visszavonási/felfüggesztési kérelemre vonatkozó türelmi ido 33
4.6.4. Visszavonási eljárás 34
4.6.5. Felfüggesztési eljárás 34

4.6.6. A felfüggesztett állapotra vonatkozó korlátozások 34
4.6.7. Visszavont Tanúsítványok Listája (CRL) és kibocsátásának gyakorisága 35
4.6.8. Visszavont Tanúsítványok Listája ellenorzési követelmények 35
4.6.9. Visszavonási állapot közlés más formái 35
4.6.10. Magánkulcs kompromittálódás speciális követelményei 35
4.7. Biztonsági audit eljárások 35
4.7.1. Naplózott esemény típusok 35
4.7.2. Napló adatok védelme 36
4.7.3. Napló adatok feldolgozása 36
4.7.4. Napló adatok tárolása 36
4.7.5. Rendkívüli eseményekrol történo értesítés 36
4.8. Adatarchiválás 36
4.8.1. A tárolt adatok típusai 37
4.8.2. Az archívum gyujtési rendszere 37
4.8.3. Az archívum megorzési idotartama 37
4.8.4. Az archívum védelme 37
4.8.5. Az archívum hozzáférését és ellenorzését végzo eljárások 37
4.9. A folyamatos üzemmenet biztosítása (katasztrófa elhárítás) 37
4.9.1. Biztonsági képesség rendkívüli üzemeltetési helyzetben 37
4.9.2. Minimális szolgáltatás rendkívüli üzemeltetési helyzetben 38
4.9.3. Üzletmenet-folytonossági Terv 38
4.10. A hitelesítés-szolgáltatási tevékenység megszüntetése 38
5. Fizikai, eljárásrendi, és humán biztonsági szabályozások 39
5.1. Fizikai biztonsági szabályozások 39
5.1.1. Hitelesíto Központok 39
5.1.2. Regisztrációs Iroda 40
5.2. Eljárásrendi szabályozások 40
5.2.1. Bizalmi munkakörök 40
5.2.2. Az egyes feladatokhoz szükséges személyzeti létszámok 41
5.2.3. A bizalmi munkakörökben elvárt azonosítás és hitelesítés 41
5.3. Humán szabályozások 41
5.3.1. Képzettségre, gyakorlatra és biztonsági ellenorzésre vonatkozó követelmények 42
5.3.2. Biztonsági háttér ellenorzésekre vonatkozó eljárások 42
5.3.3. Képzési követelmények 43
5.3.4. Továbbképzési gyakoriságok és követelmények 43
5.3.5. A felhatalmazás nélküli tevékenységek bünteto következményei 43
5.3.6. A szerzodéses alkalmazottakra vonatkozó követelmények 43
5.3.7. A személyzet számára biztosított dokumentációk 43
6. Muszaki biztonsági óvintézkedések 44
6.1. Kriptográfiai kulcspár eloállítás és aláírás-létrehozó eszköz megszemélyesítés 44
6.1.1. Kulcspár eloállítás 44
6.1.2. Aláírás-létrehozó eszköz megszemélyesítés 44

6.1.3. Az aláírás-létrehozó adat felhasználóhoz történo eljuttatása 44
6.1.4. Az Aláírók aláírás-ellenorzo adatának eljuttatása a felhasználókhoz 44
6.1.5. A Szolgáltató aláírás-ellenorzo adatainak eljuttatása a felhasználókhoz 44
6.1.6. Kulcs méretek 44
6.1.7. Elofizetoi aláírás-ellenorzo adat eloállításához használt paraméterek eloállítása 44
6.1.8. Szolgáltatói kulcsgenerálás 44
6.1.9. Kulcs felhasználási célok 44
6.2. Aláírás-létrehozó adat védelme 44
6.2.1. A HSM-re vonatkozó szabványok 44
6.2.2. A több-szereplos (“n-bol m”) magánkulcs visszaállítás ellenorzése 44
6.2.3. Aláírás-létrehozó adat letét 44
6.2.4. Aláírás-létrehozó adat mentése, duplikálása 44
6.2.5. Aláírás-létrehozó adat kriptográfiai modulba helyezése 44
6.2.6. Aláírás-létrehozó adat aktiválása 44
6.2.7. Aláírás-létrehozó adat deaktiválása 44
6.2.8. Aláírás-létrehozó adat megsemmisítése 44
6.3. Kulcspár kezelés egyéb aspektusai 44
6.3.1. Aláírás-ellenorzo adat archiválása 44
6.3.2. Aláírás-létrehozó és aláírás-ellenorzo adatok felhasználási ideje 44
6.4. Aktiválási adatok 44
6.4.1. Aktiválási adatok generálása és installációja 44
6.4.2. Aktiválási adatok védelme 44
6.4.3. Aktiválási adatok egyéb aspektusai 44
6.5. Számítógép biztonsági szabályok 44
6.5.1. Számítógép biztonság technikai követelményei 44
6.5.2. Számítógép biztonsági értékelések 44
6.6. Életciklus technikai szabályok 44
6.6.1. Rendszerfejlesztési szabályok 44
6.6.2. Biztonságkezelési szabályok 44
6.6.3. Életciklus biztonsági értékelések 44
6.7. Hálózati biztonsági szabályok 44
6.8. Kriptográfiai (HSM) modul ellenorzése 44
7. Tanúsítvány és kulcs-visszavonási profil 44
7.1. Tanúsítvány profil 44
7.1.1. Alap mezok 44
7.1.2. Tanúsítvány kiterjesztések 44
7.2. Kulcs-visszavonási profil 44
7.3. Idobélyeg profil 44
7.4. OCSP profil 44
8. HSZSZ-M adminisztráció 44
8.1. HSZSZ-M változatkezelési eljárások 44
8.1.1. HSZSZ-M változtatási eljárások 44

8.1.2. Értesítéssel változtatható elemek 44
8.1.3. Szabályzati objektumazonosítót változtató módosítások 44
8.2. Közzétételi és tájékoztatási elvek 44
8.2.1. A HSZSZ-M-ben nem tárgyalt elemek 44
8.2.2. A HSZSZ-M közzététele 44
8.3. HSZSZ-M elfogadási eljárások 44
9. Hivatkozások és Meghatározások 44
9.1. Hivatkozások 44
9.2. Meghatározások 44

1. Bevezetés

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

A Szolgáltató szolgáltatás ait a vele elofizetoi szerzodéses viszonyban álló Elofizetok részére nyújtja.

A minosített elektronikus aláírással kapcsolatos szolgáltatások (továbbiakban: szolgáltatások) keretében a Szolgáltató az Elofizetok és velük kapcsolatban álló Aláírók részére a 2001. évi XXXV. törvényben meghatározott szolgáltatások közül a következoket nyújtja:

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

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

c. idobélyegzés

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

A szolgáltatások részletezése az 1.4.4.2 pontban olvasható.

1.1. Szolgáltató adatai

Név: MÁV Informatika Kereskedelmi, Szolgáltató és Tanácsadó Korlátolt Felelosségu 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 felügyeloség:

Budapest Fováros Közigazgatási Hivatal Fogyasztóvédelmi Felügyeloség
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, szerzodéskötés, aláírás létrehozó eszköz átadása, visszavonási kérelem megerosítése, 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 munkaidoben elérheto telefonon a +36-1-457-95-78 elofizetoi közvetlen számon, vagy a +36-1-457-93-00 központi számon, valamint elektronikus levélben az ica@mavinformatika.hu címen.

A területi ügyfélkapcsolati irodák címe és elérhetosége a Szolgáltatás Internetes honlapján keresztül érheto el.

A tanúsítványok felfüggesztésére a Szolgáltató folyamatos (7x24 órás) ügyfélszolgálatot (Help Desk szolgálatot) ad. Az Ügyfélszolgálat elérheto 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 *ica@mavinformatika.hu* címeken

1.2. Alapok

1.2.1. Szabályzat célja

Jelen HSZSZ-M célja, hogy összefogja azokat az eloírásokat, adatokat és információkat, melyeket a szolgáltatással kapcsolatba kerülo felhasználói közösség tagjainak tudni kell vagy érdemes. Biztosítja a Szolgáltató muködésének átláthatóságát, s lehetové 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 idobélyeg elfogadóinak egyértelmuen meg kell tudni állapítani az elektronikus aláíráshoz, illetve az idobélyeghez kapcsolódó tanúsítvány ellenorzésének módját, az általa garantált hitelesség és biztonság mértékét és az erre vonatkozó technikai, üzleti és pénzügyi garanciákat, jogi felelosség vállalásokat.

1.2.2. Jogszabályok, szabványok

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

- 2001. évi XXXV. törvény az elektronikus aláírásról (a továbbiakban: Eat.),
- 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekrol
- 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 minosített tanúsítványok, visszavonási listák szerkezetére és tartalmára vonatkozóan:

- International Telecommunication Union X.509 “Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer”
- Minosített tanúsítványtípus minták minosített hitelesítés-szolgáltatók számára, 1.0 verzió. Hírközlési Felügyelet.
- ETSI TS 101 862 Minosített 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 – Minosített tanúsítvány profil)
- ISO 3166 szabvány

A minosített hitelesítés-szolgáltatókra vonatkozóan:

- 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekrol
- 45/2005. (III. 11.) Korm. rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatáskörérol, valamint eljárásának részletes szabályairól
- 2/2002. (IV. 26) MeHVM irányelve a minosített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekrol,
- ETSI TS 101 456 (Minosített tanúsítványokat kibocsátó hitelesítés-szolgáltatókra vonatkozó szabályozási követelmények).

Az idobélyegzésre vonatkozóan:

- RFC – 3161 (Internet X. 509 nyilvános kulcsú infrastruktúra idobélyeg protokoll)
- ETSI TS 102 023 (2003. 04) (Idobélyegzés szolgáltatókra vonatkozó követelmények)
- ETSI TS 101 861 szabvány (Idobélyegzés profil)

Az OCSP szolgáltatásra vonatkozóan:

IETF RFC 2560 szabvány

Az informatikai biztonsági követelményekre vonatkozóan:

MeH ITB 12. ajánlás, ITSEC[1], CC[2]

A kriptográfiai modulra, az aláírás-létrehozó eszközre vonatkozóan:

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

ITSEC, CC,

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

CEN 14167-3 munkacsoport egyezmény: „Védelmi profil hitelesítés-szolgáltató kulcs eloállítási 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 eloírt regisztrációs eljárásoknak megfeleloen azonosítja a jelen HSZSZ-M-t.

A dokumentum neve:	Szolgáltatási Szabályzat a Minosített 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
Idobélyegzo szoftver technikai azonosító:	T&S TSAV1.0
Elso hatálybalépés idopontja	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 jelen szabályzat a következo tanúsítványtípusok kezelését írja le:

Nyilvános körben kibocsátott minosített tanúsítványtípus (MTT)

OID: 1.3.6.1.4.1.14868.2.2.1

Nyilvános körben kibocsátott Biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelo minosített tanúsítványtípus (MTT+BALE)

OID: 1.3.6.1.4.1.14868.2.2.2

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

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

1.4. Hitelesítés szolgáltató és felhasználói közösség, alkalmazhatóság

A Szolgáltató által kibocsátott tanúsítványokat felhasználó közösség a következo:

a. a Szolgáltató regisztráló és hitelesíto egységei, a szolgáltatást muködteto elektronikus aláírásra feljogosított munkatársai

b. az Elofizetok és az Aláírók

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

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

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

d. az érintett felek

Idobélyegzés vonatkozásában a közösséget az ISZR 4. pontjában meghatározott, következo csoportok alkotják:

a. az Elofizetok
b. az idobélyegzés szolgáltató
c. az idobélyeget felhasználó (igénybevevo) fél
d. az érintett felek

Az idobélyegzés szolgáltatást minden, az ISZR 4.3 pontban meghatározott idobélyeg felhasználó igénybe veheti, függetlenül attól, hogy az idobélyeget nyilvános vagy zárt körben használja.

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

a. az Elofizetok
b. az OCSP szolgáltató
c. az OCSP válaszokat felhasználó (igénybevevo[3]) fél
d. az érintett felek

1.4.1. A Szolgáltató regisztráló és hitelesíto egységei

A Szolgáltató minosített hitelesítés-szolgáltató.

A Szolgáltató regisztráló és hitelesíto egységei:

A Hitelesítési Politika és Szabályozási Csoport, amely a szolgáltatással kapcsolatos rendek és szabályzatok kialakításáért, elfogadásáért, karbantartásáért és adminisztrációjáért felelos.

A Szolgáltató Hitelesíto Központja, amely a szolgáltatás-támogató informatikai rendszer központi eroforrásaiból, azt ezt körülvevo biztonságos fizikai környezetbol valamint az üzemeltetést és szolgáltatást ellátó személyzetbol áll.

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

Az Ügyfélkapcsolati Irodák, melyek elvégzik az igénylok (a későbbi Elofizetok) adatainak felvételét, az Elofizeto személyazonosságának megállapítását, a tanúsítvány kérelmek összeállítását és gondoskodnak az elofizetoi szerzodésben foglaltak teljesítésérol.

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

1.4.2. Elofizetok és Aláírók (Felhasználók)

Elofizeto a Szolgáltatóval szerzodéses viszonyban álló felhasználó, aki számára a Szolgáltató Tanúsítványt és/vagy idobélyeget bocsát ki. Elofizeto lehet természetes vagy jogi személy.

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

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

1.4.3. Érintett felek

Az Érintett fél (aláírás Ellenorzo) olyan természetes vagy jogi személy, aki vagy amely, az aláírt és/vagy idobélyegzett és/vagy OCSP válasszal ellátott elektronikus dokumentum fogadója, és egy adott Tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el az aláírás, és/vagy az idobélyeg és/vagy az OCSP válasz hitelességének ellenorzésekor.

1.4.4. Alkalmazhatóság

1.4.4.1. Szabályzat hatálya

A HSZSZ-M idobeli hatálya a hatálybalépés dátumával kezdodik és határozatlan idore szól. Idobeli hatálya megszunik a szolgáltatási tevékenység beszüntetésekor, illetve egy újabb szabályzat verzió hatályba lépésével.

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

A HSZSZ-M tárgyi hatálya a következokre terjed ki:

[3] Igénybevevo: az OCSP kérést elindító és a választ fogadó felhasználó

a. az 1. pontban meghatározott szolgáltatásokra

b. a Szolgáltatónak a hitelesítés szolgáltatással kapcsolatban álló összes objektumára és tárgyi eszközére

1.4.4.2. Szolgáltatás szintje

A Szolgáltató az Eat. szerinti minosített szolgáltatásokat nyújtja, melyek az alábbi összetevokbol 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. Idobélyegzés

h. OCSP szolgáltatás

1.4.4.3. Tanúsítványok alkalmazhatósága

Az elofizetoi tanúsítványok alkalmazhatóságára a következo alapszabályok érvényesek:

Engedélyezett alkalmazási lehetoségek

A kibocsátott magánkulcsok elektronikus dokumentumon kizárólag elektronikus aláírások megtételére használhatók. A magánkulcsokhoz tartozó nyilvános kulcsok az elektronikus aláírások ellenorzésére használhatók fel.

Korlátozott alkalmazási lehetoségek

Szolgáltató területi, pénzügyi, stb. korlátozásokat szabhat saját belso hitelesítési rendje szerint, amelyeket a kibocsátott elofizetoi Tanúsítványban megad.

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

Tiltott alkalmazási lehetoségek

Az elofizetoi tanúsítványok más nyilvános kulcsú tanúsítványok aláírására történo felhasználása, vagy bármilyen hitelesítés szolgáltatás nyújtásához történo 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 felelosséget az elektronikus aláírásra kibocsátott aláírás ellenorzo adat, illetve az aláírás-létrehozó adat titkosításra, vagy más, az elektronikus aláírástól eltéro felhasználására vonatkozóan.

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

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

A tanúsítvány használati lehetoségére vonatkozó fenti információk a Tanúsítványban is rögzítésre kerülnek. A tanúsítvány használati lehetoségére vonatkozó információktól bármely módon eltéro használat az Aláíró egyéni felelossége és kockázata, ahogy az ilyen módon felhasznált tanúsítvány elfogadása az érintett fél (aláírás Ellenorzo) felelossége és kockázata.

1.5. Tanúsítvány osztályok, tanúsítványtípusok és tanúsítvány fajták

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

A minosített tanúsítványok bizalmi osztályába két tanúsítványtípus tartozik:

a. nyilvános körben kibocsátott minosített tanúsítványtípus (MTT)

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

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

Szolgáltató által kibocsátott Elofizetoi tanúsítványok érvényességi ideje 1 év. Az érvényesség kezdete a kibocsátás napja.

1.5.1. Minosített tanúsítványok jellemzoi és típusai

1.5.1.1. Minosített tanúsítványok jellemzoi

Minosített tanúsítvány az Eat. 2. számú mellékletében foglalt követelményeknek megfelelo olyan tanúsítvány, amelyet minosített szolgáltató bocsátott ki. A minosített tanúsítványoknak tartalmazniuk kell az alábbiakat:

a. annak megjelölését, hogy a tanúsítvány minosített tanúsítvány

b. a Szolgáltató és székhelyének (ország-) azonosítóját

c. az Aláíró nevét (vagy egy álnevét, ennek jelzésével)

d. a tanúsítvány szándékolt felhasználásától függoen az Aláíró külön jogszabályban, a jelen Szolgáltatási Szabályzatban és az Általános Szerzodési Feltételekben (továbbiakban: ÁSZF-M-ben) meghatározott speciális jellemzoit

e. az Aláíró által birtokolt aláírás-létrehozó adatnak megfelelo aláírás-ellenorzo adatot

f. a tanúsítvány érvényességi idejének kezdetét és végét,

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 minoségét és a képviselt szervezet azonosító adatait.

1.5.1.2. Nyilvános körben kibocsátott minosített 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 minosített tanúsítványok olyan elektronikus aláírások igazolására használhatók, amelyek jogérvényesíthetosége, jogi eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg.

1.5.1.3. Nyilvános körben kibocsátott és biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelo minosített 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 minosített 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 ***minosített elektronikus aláírás***-nak kell tekinteni.

1.5.2. Tanúsítványok használati osztályainak jellemzoi

1.5.2.1. Elofizetoi tanúsítvány

Elofizetoi tanúsítvány a Szolgáltatóval szerzodéses viszonyban álló Elofizeto számára kibocsátott tanúsítvány.

Az Elofizetoi 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)

Elofizetoi tanúsítvány olyan természetes személyeknek vagy szervezeteknek kerül kiadásra, amelynél az Aláírót személyes megjelenésre, saját hitelesíto dokumentumokra és írásos nyilatkozatokra alapozott biztonsági ellenorzéssel 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 közjegyzoi okiratot is elfogad.

1.5.2.2. Szolgáltatói tanúsítvány

A szolgáltatói tanúsítványokat Szolgáltató csak saját célra bocsátja ki, a szolgáltatási termékek eloállításának biztosítására. Elofizeto 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 következokben meghatározott fajtájú minosített tanúsítványokat adhatja ki Elofizetok 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 Elofizeto és az Aláíró jellemzoen ugyanaz a személy.

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

Az álnév jelzésére a tanúsítvány CN mezojében található szöveg ’~’ (tilde) karakterrel kezdodik és végzodik (pl. CN= „~Superman~”). Amennyiben a tanúsítvány CN mezojében nem az aláíró azonosítására használt okmány(ok)ban szereplo név kerül megadásra, úgy ez a mezo álnévként kerül rögzítésre.

A tanúsítvány egyéb ellenorzött adatokat is tartalmazhat, különbözo kiterjesztés mezokben.

1.5.3.2. „Szervezeti személy” vagy „Munkatársi” tanúsítvány

„Szervezeti személy” vagy „Munkatársi” típusú tanúsítványokat természetes személy igényelhet egy adott szervezet alkalmazottjaként és/vagy tisztségviselojeként.

Ebben az esetben az Elofizeto a szervezet, az Aláíró a szervezetet képviselo személy. Az Elofizetoi Szerzodésben a szervezet által vállalt kötelezettségek egyetemlegesen érvényesek a szervzetet képviselo Aláíróra.

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

Az álnév jelzésére a tanúsítvány CN mezojében található szöveg ’~’ (tilde) karakterrel kezdodik és végzodik (pl. CN= „~Superman~”). Amennyiben a tanúsítvány CN mezojében nem az aláíró azonosítására használt okmány(ok)ban szereplo név kerül megadásra, úgy ez a mezo álnévként kerül rögzítésre.

A tanúsítvány egyéb ellenorzött adatokat is tartalmazhat, különbözo kiterjesztés mezokben.

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 elérhetové teszi.
3. A Szolgáltató jogi személy.
4. A Szolgáltató rendszeresen felülvizsgálja és újra kiadja HSZSZ-M-ét.
5. A Szolgáltató mindenkor az Elofizeto által szolgáltatott és az Ügyfélkapcsolati Irodák által elfogadott adatok alapján bocsátja ki a tanúsítványokat. A Szolgáltató a tanúsítvány kibocsátását követoen a tanúsítvány adataiban változást nem eszközölhet.
6. A Szolgáltató a Tanúsítványtárában teszi közzé az általa kibocsátott, felfüggesztett és visszavont elofizetoi tanúsítványokat. A Tanúsítványtár, a Tanúsítványok Visszavonási Listája (CRL) és az OCSP szolgáltatás elérhetoségét a Szolgáltató 99,9%-os rendelkezésre állással biztosítja úgy, hogy az elérhetoség kiesése esetenként nem lépheti túl a 3 órás idotartamot.
7. A Szolgáltató kötelezettséget vállal arra, hogy a regisztrációt követo napokban, de legkésobb 30 munkanapon belül a tanúsítvány kiadására intézkedik és errol az Elofizetot értesíti.
8. A Szolgáltató a szolgáltatások muködtetése és menedzselése során az ügyfélkapcsolati tevékenységet Ügyfélkapcsolati Irodák által biztosítja.
9. A Szolgáltató 99,9%-os rendelkezésre állással biztosítja a visszavonás kezelési szolgáltatást minden érdekelt fél számára még rendkívüli üzemeltetési helyzetben is. 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 elérhetové teszi a jogszabály szerinti nyilvántartásokat és a tanúsítvány kibocsátására vonatkozó saját szabályzatait.
11. A Szolgáltató a lejárat elott 15 nappal értesítést küld a lejáró tanúsítványokról az Elofizeto részére.
12. Szolgáltató a Tanúsítványban feltünteti az Elofizetoi Szerzodésben rögzített, a tanúsítvány felhasználhatóságával kapcsolatos korlátozásokat.
13. A Szolgáltató felfüggeszti vagy visszavonja a tanúsítványt és ezt közzéteszi ha a 4.6.1 fejezetben részletezett körülmények ezt indokolják
14. Szolgáltató megorzi a tanúsítványokkal kapcsolatos adatokat és az ahhoz kapcsolódó személyes adatokat legalább a tanúsítvány érvényességének lejáratától számított 10 évig, illetoleg – amennyiben ezen idoszakban az elektronikus aláírással vagy az azzal aláírt elektronikus dokumentummal kapcsolatosan jogvita merül fel és azt a Szolgáltatónak írásban bejelentették – a jogvita jogeros lezárásáig. Ugyanezen határidoig olyan eszközt is biztosít, mellyel a kibocsátott tanúsítvány tartalma megállapítható.
15. Ha a Szolgáltató be kívánja fejezni tevékenységét, errol legalább hatvan nappal korábban értesíti az Elofizetoket és a Nemzeti Hírközlési Hatóságot. A bejelentés idopontjától kezdve a Szolgáltató nem bocsáthat ki új Tanúsítványt. A Szolgáltató a tevékenység befejezése elott 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 legkésobb 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 hitelesíto központok („CA”-k) feladata

A Szolgáltató által muködtetett hitelesíto központok feladata a tanúsítványok eloállítása és az idobélyegzés, valamint a visszavonási listák aláírásával közremuködés a visszavonási állapot közzétételében.

A tanúsítványok eloállítása 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 közremuködés 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. szintu „Root CA” alapveto feladata és hatásköre a 2. szintu „Produktív CA” és az idobélyegzo egység hitelesítése, ezen belül a feladatok tételesen a következok:

1. Saját (szolgáltatói) kulcspár generálása és tanúsítvány eloállítása önhitelesítéssel, magánkulcsának fokozott biztonságú védelme
2. További szolgáltatói kulcspárok és tanúsítványok eloállítása
3. A 2. szintu hitelesíto központok ("Produktív CA"-k) hitelesítési kérelmeinek fogadása és ellenorzése, részükre tanúsítványok eloállítása, hitelesítése
4. Tanúsítvány eloállítása és hitelesítése az idobélyegzo 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. szintu „Produktív CA" Hitelesíto Központ alapveto feladata és hatásköre a Regisztrációs Iroda ("RA") és az általa regisztrált Elofizetok tanúsítványainak hitelesítése:

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

2.1.1.2. A Regisztrációs Iroda (RA) feladatai és hatásköre

A Regisztrációs Iroda fo feladata a hitelesítés-szolgáltatás (regisztráció, felfüggesztés és visszavonás kezelés) és az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése. Egyúttal közremuködik az elofizetoi tanúsítvány eloállítás, kibocsátás és visszavonási állapot közzététele szolgáltatásokban.

1. a tanúsítvány kibocsátásához szükséges ellenorzések sikeres lefolytatása után a tanúsítvány kibocsátás elindítása a Hitelesíto Központnál, (visszautasítja a tanúsítvány kiadását, amennyiben a tanúsítvány-igénylés nem felel meg az elvárt feltételeknek)
2. fogadja a Hitelesíto Központtól kapott elofizetoi tanúsítványokat és ellenorzi azok hitelességét és sértetlenségét,
3. kezdeményezi a tanúsítványok elküldését a Tanúsítványtárba
4. elokészíti a biztonságos aláírás-létrehozó eszközt az aláírás-létrehozó eszközön történo kulcspár generáláshoz
5. megszemélyesíti az aláírás-létrehozó eszközt és azt személyesen eljuttatja az Ügyfélkapcsolati Irodához
6. eloállítja a kezdeti aktivizáló adatot (PIN kódot), majd azt az aláírás-létrehozó eszköztol elkülönítve eljuttatja az Ügyfélkapcsolati Irodához,
7. (szoftveres úton történo kulcspár generálás esetén biztonságos módon eljuttatja a kulcspárt az aláírás-létrehozó eszközbe, olyan biztonságos útvonal kiépítésével, mely kriptográfiai mechanizmusok felhasználásával forrás hitelesítést, sértetlenséget és bizalmasságot biztosít,
8. biztonságos módon megsemmisíti az eloállított magánkulcs aláírás-létrehozó eszközön kívüli összes példányát, miután az Aláíró részére eloállított kulcspárt elhelyezte az aláírás-létrehozó eszközben),
9. formai szempontból ellenorzi 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 idobélyegzo egység feladata

1. a kéro által kezdeményezett biztonságos csatornán keresztül fogadja az idobélyegzési kérelmeket,
2. azonosítja és hitelesíti az idobélyeg kérot, ellenorzi a kérelem szabályosságát,
3. eloállítja az idobélyeget, amennyiben a Szolgáltató rendszere a pontos idot biztosítani tudja,
4. a kéro által kezdeményezett biztonságos csatornán keresztül elküldi az idobélyeget a felhasználónak szabványos formában,
5. ellenorzi az idobélyegzo szerver belso órájának pontosságát;
6. amennyiben az óra a pontossági határon kívülre kerül, az idobélyegzo szolgáltatást leállítja, és hibaüzenetet küld az Elofizetok felé,

7. az idobélyegzo szerver belso órájának az ISZR-ben eloírt pontosságú szinkronizációja hiteles külso UTC ido alapján történik,
8. a belso óra pontosságának folyamatos ellenorzése,
9. az idobélyeg aláíró kulcs fokozott biztonságú eloállítása és tárolása a 2/2002. (IV.26) MeHVM irányelvnek megfeleloen,
10. az idobélyegzéssel kapcsolatos események rögzítése, naplózása és archiválása.

2.1.1.4. Az OCSP egység feladata

1. a kéro által kezdeményezett biztonságos csatornán keresztül fogadja az OCSP kérelmeket,
2. azonosítja és hitelesíti az OCSP állapot kérot, ellenorzi a kérelem szabályosságát,
3. eloállítja az OCSP választ, amennyiben a Szolgáltató rendszere a pontos idot biztosítani tudja,
4. a kéro által kezdeményezett biztonságos csatornán keresztül elküldi az OCSP választ a felhasználónak szabványos formában,
5. ellenorzi az OCSP szerver belso órájának pontosságát;
6. amennyiben az óra a pontossági határon kívülre kerül, az OCSP szolgáltatást leállítja, és hibaüzenetet küld az Elofizetok felé,
7. az OCSP szerver belso órájának az ISZR-ben eloírt pontosságú szinkronizációja hiteles külso UTC ido alapján történik,
8. a belso óra pontosságának folyamatos ellenorzése,
9. az OCSP válasz aláíró kulcs fokozott biztonságú eloállítása és tárolása a 2/2002. (IV.26) MeHVM irányelvnek megfeleloen,
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 Igénylo megfelelo tájékoztatásáról és azonosításáról
2. ellenorzi a 3.1 pontban és az ÁSZF-M-ben eloírt adatszolgáltatási követelmények szerint megadott adatok alapján a szolgáltatást igénylo ügyfél személyazonosságát és az Aláíró adatait
3. meghatározza a Tanúsítványba kerülo adatokat, ellenorzi az Igénylo által átadott dokumentumok valódiságát, érvényességét, sértetlenségét és hitelességét,
4. lehetoség szerint ellenorzi a dokumentumok érvényességét, valódiságát valós ideju nyilvántartásokban is,
5. elokészíti az Elofizetoi Szerzodést
6. elszámolja és kiszámlázza a szolgáltatás ok ellenértékét,
7. nyilvántartásba veszi a regisztráció során felvett adatokat és megorzi azokat.
8. bizalmas információként kezeli az Elofizeto 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 Elofizetot tanúsítványa lejáratát megelozoen 15 nappal
11. az Aláíró adatainak változása és tanúsítvány megújítási kérelem esetén ellenorzi 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. ellenorzi 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 Politika és Szabályozási Csoport feladatai és hatásköre

A Hitelesítési Politika és Szabályozási Csoport a Szolgáltató a szolgáltatást nyújtó szervezeti egységtol függetlenül muködik. Kötelessége a Szolgáltató és felhasználó Közösség igényeinek felmérése és folyamatos követése, ezek alapján a közösség muködésére vonatkozó alapelvek, politikák lefektetése, s ebbol 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 Elofizetoi Szerzodések és a Biztonsági Szabályzat, készítése és rendszeres karbantartása változatkövetéssel.

A Hitelesítési Politika és Szabályozási Csoport feladatai tételesen a következok:

1. A hitelesítési-, és idobélyegzési szolgáltatási rendek elkészítése és karbantartása.
2. A hitelesítés-szolgáltatási szabályzatok és az általános szerzodési feltételek elkészítése és karbantartása.
3. A hitelesítési rendek és szabályzatok közötti összhang biztosítása.
4. A szolgáltatói szabályzatok verzióinak nyilvántartása és megorzése.
5. Nyilvános szabályzatok publikálása.
6. A regisztrációs folyamat szabályozása, ellenorzése, 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 Elofizeto és az Aláíró feladatai és hatásköre

Az Elofizeto és az Aláíró kötelessége a Szolgáltató szerzodéses feltételeinek és szabályzatainak megfeleloen eljárni a szolgáltatás igénybevétele során. Ennnek során az Elofizeto 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 Elofizeto a regiszrtráció során a Tanúsítvány kiadásához szükséges adatokat ellenorizni,
4. az Aláíró biztosítani az aláírás-létrehozó eszközének és adatának, valamint a PIN kódjának védelmét,
5. az Elofizeto, illetve az Aláíró 3 (három) munkanapon belül jelezni Szolgáltatnál a regisztráció során felvett adataiban történo változásokat, különös tekintettel a Tanúsítványba foglalt adatokra,
6. az Aláíró az aláírás-létrehozó adatát csak az elofizetoi szerzodésben rögzített korlátozásoknak megfeleloen használhatja,
7. az Aláíró tudomásul venni, hogy magánkulcsának védelme és az elektronikus aláírás készítése kizárólag a saját felelossége, ezért ezzel - így különösen a magánkulcsának illetéktelen harmadik személyhez kerülésével - kapcsolatban a Szolgáltatót semmiféle felelosség nem terheli,
8. az Elofizeto az ÁSZF-M módosításáról szóló értesítést követoen 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 Elofizeto a Tanúsítvánnyal ellátott elektronikus dokumentummal kapcsolatos jogvita megindulásáról köteles haladéktalanul tájékoztatni a Szolgáltatót,
12. az idobélyeget felhasználók kötelesek a kért idobélyeg vétele után meggyozodni arról, hogy az idobélyeget a Szolgáltató elektronikusan aláírta, az aláírás az idobélyegzésre szolgáló kulccsal történt-e és a hozzátartozó tanúsítvány érvényes-e;
13. az OCSP válasz felhasználók kötelesek a kért OCSP válaszok vétele után meggyozodni 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 minosül, és viseli ennek jogkövetkezményeit;

2.1.3. Érintett fél feladatai és hatásköre

Az Érintett félnek a Szolgáltató szabályzataiban leírtaknak megfeleloen a legnagyobb gondossággal kell eljárnia az Elektronikus aláírás és a tanúsítvány elbírálásakor, ezen belül:

1. az Elektronikus aláírás elfogadása elott meg kell értenie az Elektronikus aláírással kapcsolatos technikai, jogi, biztonsági és egyéb vonatkozásokat,
2. meg kell ismernie Szolgáltató nyilvánosan elérheto szabályzatait (HSZSZ-M, ÁSZF-M) és az Elektronikus aláírással ellátott dokumentum alapján végzett bármilyen tevékenység a Szolgáltató szabályzatának elfogadását jelenti,

3. az Elektronikus aláírás ellenorzését el kell végeznie az Aláíró Tanúsítványának segítségével, meggyozodve az üzenet eredetiségérol és az aláírás valódiságáról,
4. a Tanúsítványban feltuntetett azonosító alapján, és egyéb adatok, törvényesen rendelkezésre álló módszerek segítségével az Aláíró személyérol egyértelmuen meg kell gyozodnie,
5. a tanúsítvány érvényességét és hatályosságát ellenoriznie kell a nyilvánosan elérheto Tanúsítványban,
6. el kell végeznie a teljes tanúsítási lánc ellenorzését az alábbiak szerint:
   - 6.1 a tanúsítvány kibocsátójának azonosítója alapján a Kibocsátó kilétérol meg kell gyozodnie;
   - 6.2 a Szolgáltató (Kibocsátó) Tanúsítványának segítségével az Aláíró Tanúsítványának integritásáról meg kell gyozodnie;
   - 6.3 a tanúsítvány állapotát ellenoriznie kell a tanúsítvány visszavonási listák (CRL) áttanulmányozásával vagy OCSP szolgáltatás igénybe vételével;
   - 6.4 át kell tanulmányoznia a tanúsítvány összes attribútumát, és az adott tranzakcióra vonatkozó eloírásoknak, valamint józan megfontolásoknak megfeleloen 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 idobélyeget aláíró kulcs tanúsítványának az Érintett fél által történo ellenorzésére vonatkozóan általában érvényesek a 2.2.3 pontban leírt, a tanúsítvány ellenorzésre vonatkozó szabályok.
9. Egy idobélyeggel ellátott állomány átvétele után az Érintett félnek ellenoriznie kell a Szolgáltató általi aláírás megtörténtét, az Szolgáltató idobélyeget 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 történo ellenorzésére vonatkozóan általában érvényesek a 2.2.3 pontban leírt, a tanúsítvány ellenorzésre vonatkozó szabályok.
11. Egy OCSP válasszal ellátott állomány átvétele után az Érintett félnek ellenoriznie kell 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. Ha az ellenorzés a tanúsítvány érvényességének lejárta után történik, akkor az Eat. 9.§ (7. bek.) alapján a szolgáltatónál 10 évig, illetve az aláírt és/vagy idobélyegzett és/vagy OCSP válaszzal elátott dokumentummal kapcsolatban felmerült jogvita lezárásáig megorzött, a tanúsítványokkal kapcsolatos elektronikus információkat és ahhoz kapcsolódó személyes adatokat elo lehet keresni és a tanúsítvány érvényességét ellenorizni kell. A tanúsítvány tartalmának megállapításához a Szolgáltatónak kell a megfelelo eszközt biztosítania.

2.2. Felelosségek

2.2.1. A Szolgáltató felelossége

A Szolgáltató azzal, hogy aláír egy, a jelen HSZSZ-M 1.5 pontja szerint meghatározott tanúsítványt, idobélyeget, illetve OCSP választ – és ezzel jelzi az 1.4 pontban meghatározott felhasználó közösség felé ezen HSZSZ-M használatát – azért vállalja a felelosséget, hogy a tanúsítvány eloállítása, kibocsátása, közzététele, visszavonása, a Visszavonási Lista közzététele, az idobélyegzés és OCSP válaszadás tevékenységek a jelen HSZSZ-M-ben eloírtaknak teljes mértékben megfelelnek, és a Szolgáltató megteszi a szükséges intézkedéseket ahhoz, hogy a Szolgáltató maga és az Elofizetok is a jelen HSZSZ-M eloírásainak megfeleloen járjanak el.

A Szolgáltató a vele szerzodéses jogviszonyban nem álló harmadik személlyel szemben a Magyar Köztársaság Polgári Törvénykönyvérol szóló 1959. évi IV. törvény 339. §-a szerint, az Elofizetovel szemben pedig a szerzodésszegésért való felelosség szabályai szerint felelos az elektronikus aláírással aláírt elektronikus dokumentummal okozott kárért, ha megszegte a HSZSZ-M-ben, az ÁSZF-M-ben vagy az elofizetoi szerzodésben eloírtakat, 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 felelosségvállalás mértékét, mely tanúsítvány típusonként és egyedi tanúsítványonként is maximált összegu, az Elofizetoi Szerzodésben kell rögzeni.

A Szolgáltató nem vállal felelosséget, ha a Szolgáltató által kibocsátott tanúsítvány a jelen HSZSZ-M-ben eloírtaktól eltéro módon kerül felhasználásra. Így a Szolgáltató nem felelos az olyan károkért, melyek abból adódtak, hogy az Érintett fél a tanúsítványok ellenorzése és felhasználása során nem a hatályos jogszabályok és Szolgáltató HSZSZ-M-e szerint járt el, illetve nem tanúsította a tole elvárható gondosságot.

A Szolgáltató azáltal, hogy az Elofizetok részére tanúsítványokat, idobélyegeket vagy OCSP válaszokat bocsát ki, semmilyen körülmények között sem tekintheto az Elofizetok vagy az érintett felek ügynökének, megbízottjának, képviselojének, vagy bármilyen más, az Elofizetoi Szerzodésben meghatározottól eltéro funkciójú partnerének a hitelesítési tevékenysége vonatkozásában.

2.2.2. Az Elofizeto és az Aláíró felelossége

Az Elofizetonek és az Aláírónak felelossége áll fenn a regisztráció során megadott adatainak valódiságával kapcsolatban.

Az Elofizetonek kártérítési felelossége 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 Elofizeto felelos azért, ha magánkulcsát nem a HSZSZ-M-ben, az ÁSZF-M-ben és a vonatkozó jogszabályokban meghatározott módon és célra használta.

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

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

b. az aláírás-létrehozó adatnak illetéktelen személy tudomására jutásáról vagy elvesztésérol;

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

d. a tanúsítvánnyal ellátott elektronikusan aláírt elektronikus dokumentummal, idobélyeggel vagy OCSP válasszal kapcsolatos jogvita megindulásáról.

Az Elofizeto és az Aláíró felelos az aláírás-létrehozó eszköz biztonságos megorzéséért, az aláírás-létrehozó eszköz adat és a PIN kód illetéktelenek tudomására jutásának megakadályozásáért.

Az idobélyeget kéro fél felelos az idobélyeg aláírás helyességének és az idobélyeg aláíró kulcs Tanúsítványa érvényességének az idobélyegzett állomány vételekor elvégzendo, a 2.1.2 pont szerinti ellenorzésért.

Az OCSP választ kéro fél felelos az OCSP válasz aláírás helyességének és az OCSP választ aláíró kulcs Tanúsítványa érvényességének az OCSP választ tartalmazó állomány vételekor elvégzendo, a 2.1.2 pont szerinti ellenorzésért.

A Szolgáltató nem vállal felelosséget a magánkulcs hordozó elvesztésébol, vagy a kulcs biztonságának egyéb módon történo sérülésébol, elvesztésébol, illetve a PIN kód illetéktelen tudomásra jutásból származó károkért.

2.2.3. Érintett fél felelossége

Az Érintett fél felelos az elektronikus aláírás és a Szolgáltató által kibocsátott tanúsítványok elfogadása során tanúsított körültekinto ellenorzésért, valamint a Szolgáltató nyilvánosan elérheto HSZSZ-M-e rá vonatkozó részének megismerésért.

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

2.3. Az anyagi felelosség mértéke

A Szolgáltató anyagi felelosségének mértékérol, illetve annak korlátairól az ÁSZF-M rendelkezik.

A Szolgáltató az anyagi felelosségre vonhatóság, az általa okozott károkkal kapcsolatos saját felelosség, illetve a neki okozott károkért járó kártérítés megállapíthatósága, dokumentálása és bizonyíthatósága érdekében naplózza tevékenységeit, védi a naplóbejegyzések sértetlenségét és hitelességét, valamint hosszú távon megorzi azokat (lásd: 4.6.7 és 4.8 fejezetek).

2.4. Értelmezés és alkalmazás

2.4.1. Irányadó jog

A Szolgáltató tevékenységét a mindenkor hatályos magyar jogszabályoknak megfeleloen végzi. Szerzodéseire, szabályzataira és azok teljesítésére a magyar jog az irányadó és azok a magyar jog szerint értelmezendok.

A Szolgáltató tevékenységére elsosorban a következo jogszabályok mérvadók:

2001. évi XXXV. törvény (Eat.),

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

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

15/2001. (VIII. 27.) MeHVM rendelet az elektronikus aláírási termékek tanúsítását végzo szervezetekrol, illetve a kijelölésükre vonatkozó szabályokról,

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

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

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

Ezeken túlmenoen 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 védelmérol és a közérdeku 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, megszunés, értesítések

2.4.2.1. Érvénytelenség

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

A jelen HSZSZ-M minden olyan rendelkezése, amelyek a felelosségek, a kötelezettségek, garanciák és a kártérítés korlátaira vonatkoznak, azok függetlenül más intézkedésektol, önmagukban értelmezendok és érvényesítendok.

2.4.2.2. Hatályosság

A HSZSZ-M és az ÁSZF-M a felhasználói közösség résztvevoinek valamennyi kötelezettségét, felelosségét és jogát tartalmazza. A HSZSZ-M egyetlen pontja sem értelmezheto a jelen dokumentumba foglalt értelmezéstol eltéroen. A HSZSZ-M csak írott és hitelesített formában módosítható, a Nemzeti Hírközlési Hatóság által vezetett nyilvántartásban való átvezetés mellett.

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

2.4.2.3. Megszunés

A HSZSZ-M a Szolgáltató muködésének befejezésével tekintendo megszuntnek.

2.4.2.4. Értesítések

Az Elofizetok, az Aláírók és az Érintett felek vagy bármely harmadik fél az Ügyfélkapcsolati Irodát munkanapokon megkeresheti ügyfélfogadási idoben 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 történo kommunikáció esetében a feladó nevét és elérhetoségét fel kell tüntetni és a feladónak a küldeményt hitelesítenie kell.

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

2.4.3. Vitás kérdések kezelése

Bármely vitás kérdés felmerülése esetén az Elofizetonek kötelessége a Szolgáltató haladéktalan értesítése és teljesköru tájékoztatása a kérdés minden vonatkozását érintoen, a vita jogi útra terelése elott.

Panaszt az Elofizetot nyilvántartó Ügyfélkapcsolati Irodán vagy az Ügyfélszolgálatnál lehet írásban vagy szóban eloterjeszteni. A panaszt a Szolgáltató az eloterjesztéstol számított 10 munkanapon belül kivizsgálja.

A jogviták esetén követendo 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 Elofizetokre vonatkozó hatályos szolgáltatási díjak az Elofizetoi Szerzodésben kerülnek rögzítésre.

A Szolgáltató a következo pontokban ismertetett díjtípusokat ajánlja fel az Elofizetonek.

2.5.1. Tanúsítvány kibocsátás

Szolgáltató a kibocsátott és megújított tanúsítványokért éves fenntartási díjat számol fel az Elofizeto felé, amely tartalmazza a tanúsítványok kibocsátásának (illetve megújítás esetén megújításának) és Tanúsítványtárban történo közzétételének díját az érvényesség idotartamára, 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. Idobélyegzés

A Szolgáltató az idobélyegek kibocsátásáért az erre vonatkozó szerzodés keretében meghatározott díjat számol fel.

2.5.5. OCSP szolgáltatás

A Szolgáltató az OCSP szolgáltatásért az Elofizetoi Szerzodésben meghatározott díjat számol fel.

2.5.6. Egyéb szolgáltatásokra vonatkozó díjak

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

2.5.7. Visszatérítési elvek

Az Elofizeto a számára kibocsátott tanúsítvány éves fenntartási díjának visszatérítésére a következo esetekben jogosult:

a. a kibocsátott tanúsítvány valamely adata a Szolgáltató hibájából fakadóan nem megfelelo,

b. a kibocsátott tanúsítvány, magánkulcs és aktivizáló adat nem összetartozó,

c. a kibocsátott aláírás-létrehozó eszközön szereplo adatok a Szolgáltató hibájából fakadóan nem megfelelok,

d. a kibocsátott aláírás-létrehozó eszköz, az aktivizáló kód és a kulcsok nem összetartozók,

e. a Szolgáltató bizonyítottan nem tartja be valamely kötelezettségét Elofizeto Tanúsítványának kezelésekor.

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

A tanúsítvány kibocsátását, illetve megújítását követo 30 naptári napon túl az Elofizeto kizárólag csak a Szolgáltató bizonyított szerzodés- vagy kötelezettségszegése esetén jogosult díjvisszafizetésre.

A Szolgáltató egyéb tevékenységeiért számlázott díjak esetében díjvisszafizetésre nem köteles.

2.6. Közzététel

2.6.1. Szolgáltatói információk közzététele

A Szolgáltató gondoskodik arról, hogy az általa kibocsátott tanúsítványok, a tanúsítványok használatának feltételei és egyéb közérdeku szolgáltatói információk az Elofizetok és az érintett felek részére folyamatosan rendelkezésére álljanak:

a. tanúsítvány típusok

b. tanúsítványok használatára vonatkozó ismertetok, szabályzatok, nyomtatványok

c. kibocsátott elofizetoi és szolgáltatói tanúsítványok
d. felfüggesztett és visszavont elofizetoi és szolgáltatói tanúsítványok
e. szolgáltatói közlemények

A Szolgáltató a szolgáltatói információkat Internetes honlapján keresztül teszi elérhetové. Szolgáltatónak csak saját elektronikus aláírásával ellátott dokumentumai tekinthetok eredetinek. A dokumentumok nyomtatott változatai semmilyen formában sem tekinthetok hivatalos példánynak vagy hiteles másolatnak.

2.6.2. A közzététel gyakorisága

A Szolgáltató a kibocsátott elofizetoi tanúsítványokat a Tanúsítványtárban 24 órán belül közzéteszi.

A Szolgáltató általa muködtetett hitelesíto központok szolgáltatói tanúsítványait a Tanúsítványtárában 24 órán belül közzéteszi.

A Visszavont Tanúsítványok listáját a 4.6.7 pontnak megfelelo gyakorisággal teszi közzé.

A Szolgáltató a HSZSZ-M-ben és az ÁSZF-M-ben tervezett változásokról a hatályba lépést megelozoen 30 nappal tájékoztatja a Nemzeti Hírközlési Hatóságot.

2.6.3. Elérési szabályok

A Szolgáltató minden Elofizeto és Érintett fél számára elérhetové teszi a szolgáltatás Internetes honlapját, ezen keresztül Tanúsítványtárát és tanúsítvány Visszavonási Listáját olvasás céljából. A Tanúsítványtárban keresési lehetoséget biztosít a tanúsítvány sorszáma és az azonosító adatai alapján.

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

2.6.4. 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 elérhetoségét 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 idotartamot.

2.7. A megfeleloség vizsgálata

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

A Nemzeti Hírközlési Hatóság a Szolgáltató bejelentése alapján a jelen dokumentumban megnevezett tanúsítványtípusokat nyilvántartásába felvette.

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

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

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

a. a saját szervezetén belüli belso auditor szervezettel
b. független külso auditor céggel

A Szolgáltató a szolgáltatási rendszerének következo elemeit auditáltatja:

a. Az elofizetoi és szolgáltatói minosített tanúsítványok kezeléshez és az idobélyegzéshez felhasznált elektronikus aláírási termékeit
b. Az elofizetoi és szolgáltatói minosített tanúsítványok kezeléshez, az idobélyegzéshez és az OCSP szolgáltatáshoz használt rendszereit és módszereit

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

2.7.1. Vizsgálatok gyakorisága

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

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

A Nemzeti Hírközlési Hatóság a jogszabályoknak megfeleloen évente átfogó helyszíni ellenorzést végez.

A Szolgáltató a külso, illetve a saját ellenorzo szervezete által végzett belso vizsgálatokat a Biztonsági Szabályzatában megjelölt rendszerességgel végezteti, illetve végzi.

2.7.2. Az átvizsgáló szervezet megnevezése/jellemzoi

A belso hitelesítési tevékenységre és az informatikai biztonságra vonatkozó auditot a Szolgáltató informatikai biztonsági menedzsere, a külso 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 minosítési kérelmének beadása elott az EDIPORT Kft. végezte el. Az auditálás folyamatát és eredményét a Nemzeti Hírközlési Hatóság szakértoi listájában szereplo Erdosi Péter Máté ellenorizte.

2.7.3. Hiányosságok kezelése

A Nemzeti Hírközlési Hatóság által a rendszeres helyszíni ellenorzések során feltárt esetleges hiányosságokat a Szolgáltató késlekedés nélkül megszünteti a vizsgálatot végzo 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 szabályzat

2.8.1. Bizalmas információk

Szolgáltató az elofizetoi adatokat kizárólag csak a hitelesítési-szolgáltatással összefüggésben használhatja fel.

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

a. A fontos bejegyzéseket védi az elveszéstol, tönkretételtol és hamisítástól

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

c. nyilvántartásba veszi az Elofizetovel aláírt szerzodést, beleértve az Elofizeto hozzájárulását az alábbiakhoz:

- hozzájárulás a szolgáltatások során felhasznált adatok hitelesítés-szolgáltató által történo nyilvántartásba vételéhez
- hozzájárulás a nyilvántartásba vett adatok harmadik félhez történo 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 Elofizetore és az Aláíróra vonatkozó adatok bizalmas kezeléséről, kivéve, ha felfedésükhöz ok maguk[4] hozzájárulnak, vagy ha bíróság, illetve egyéb jogi követelmény ezt eloírja,

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

A bizalmasság szempontjából legmagasabb érzékenységi szintet képviselo 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 következo bizalmas adatköröket kezeli:

[4] vagy nevükben az Elofizeto

a. a Szolgáltató üzleti titkai

b. az Elofizeto Társaságok által a Szolgáltatónak átadott üzleti titkok

c. az Elofizetok és a Szolgáltató munkatársainak, valamint 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 szerzodo fél sem jogosult az Elofizetoi Szerzodés teljesítése kapcsán tudomására jutott bármely adatot, tényt, információt, tervet vagy dokumentumot a másik fél elozetes írásbeli hozzájárulása nélkül harmadik személynek átadni.

A személyes adatok vonatkozásban az 1992. évi LXIII. törvény a személyes adatok védelmérol és a közérdeku 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 Elofizetok és az Aláírók személyes adatait csak a közöttük fennálló Elofizetoi Szerzodéssel összhangban levo célokra használhatja fel, harmadik félnek azokat az Elofizetok 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 – Elofizeto és Szolgáltató ilyen irányú megállapodása esetén - nyilvánosságra kerül, másik részét a Szolgáltató védett módon tárolja az Elofizeto és az Aláíró azonosságának igazolása és egyéb adatszolgáltatási kötelezettségei céljából.

2.8.2. Nem bizalmas információk

A Szolgáltató a regisztrációs urlapon külön jelöli mindazon adatokat, melyek a Tanúsítványtárban hozzáférheto elofizetoi 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 rendelkezok részére

A Szolgáltató az elektronikus aláírás felhasználásával elkövetett buncselekmények felderítése vagy megelozése céljából, illetoleg nemzetbiztonsági érdekbol – 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 Elofizetot sem az Aláírót nem tájékoztathatja.

2.8.5. Információszolgáltatás polgári eljárás keretében

A Szolgáltató a tanúsítvány érvényességét érinto polgári peres, illetve nem peres eljárás során - az érintettség igazolása esetén - az Aláíró személyazonosságát igazoló adatokat átadhatja az ellenérdeku peres félnek vagy képviselojének feltárhat bizalmas felhasználói információkat, illetoleg azt közölheti a megkereso bírósággal az Eat. 11.§ paragrafusa alapján.

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

2.8.6. Feltárás tulajdonos kérésére

Szolgáltató a törvényi meghatalmazással rendelkezok részére történo adatszolgáltatáson túl más Társaság üzleti titkát, az Elofizetok és az Aláírók nem nyilvános személyes adatait csak az Illeto Társaság illetve Elofizeto 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 fuzodo jogok

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

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

A visszavonási információ a Szolgáltató tulajdonát képezi.

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

A Tanúsítványban szereplo megkülönbözteto név használatára a megnevezett Tulajdonos jogosult.

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

A Szolgáltató szabályzatai, szerzodéses feltételei a Szolgáltató tulajdonát képezik.

A Tanúsítványban szereplo hitelesíto azonosító a Szolgáltató tulajdonát képezi.

3. Azonosítás és hitelesítés

3.1. Regisztráció

A Szolgáltató a tanúsítvány igényléséhez szükséges regisztráció során:

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

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

Ha egy Igénylo csak idobélyegzés szolgáltatást igényel, a kezdeti regisztráció egyszerusített eljárással történik a 3.1.9 pont szerint.

3.1.1. Nevek típusa

A tanúsítványokban szereplo névmegadás az ITU-T[5] X.500 ajánlásának felel meg.

3.1.2. Nevek szemantikája

A tanúsítványban szerepeltetendo nevek megadásakor a következo szabályok szerint kell eljárni:

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

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

3.1.3. Nevek egyedisége

A Szolgáltató biztosítja tanúsítványtárában a tulajdonosazonosítók egyediségét. Errol elsodlegesen az Aláíró nevének a névmegadásban való szerepeltetése gondoskodik. A Szolgáltató a név azonosító kiosztásakor ellenorzi, hogy az adott név szerepel-e egy más személy részére korábban kibocsátott Tanúsítványban. Ha szerepel, és a tanúsítvány név azonosítójának egyéb mezoi sem biztosítják az egyediséget, akkor a Szolgáltató fenntartja magának a jogot a név olyan megváltoztatására, amely továbbra is jellemzo az Aláíróra, de biztosítja a megkülönböztethetoséget.

3.1.4. Név igénylési viták feloldása

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

Az Elofizetonek álnévre való igényét a regisztrációs urlapon, az ott rendszeresített módon kell jeleznie.

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

3.1.5. Védjegyek elismerésének és hitelesítésének módszere

A tanúsítványkérelemmel az Elofizeto kifejezi, hogy a benne foglalt nevek, védjegyek, egyéb adatok nem sértik harmadik fél jogait. Szolgáltatónak nem kötelessége a védjegyek jogos használatának ellenorzése, és nem vállal közvetíto vagy döntnöki szerepet ilyen jellegu viták feloldásában. Szolgáltató nem garantálja Elofizetok számára védjegyeik feltüntetését a Tanúsítványban.

3.1.6. Az aláírás-létrehozó adat birtoklás ellenorzésének módszere

Az Aláíró számára az aláírás-létrehozó adat és az aláírás-ellenorzo adat (kriptográfiai kulcspár) eloállítása 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 ese-

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

tében) áll elo, ezért az aláírás-létrehozó adat és az aláírás-ellenorzo adat birtoklásának és egymáshoz tartozásának ellenorzésére nincs szükség, csupán az aláírás-létrehozó eszköz átvételének igazolása szükséges. Az aláírás-létrehozó eszköz személyes átvételénél az Elofizeto aláírásával igazolja az aláírás-létrehozó eszköz és a PIN kód átvételét.

3.1.7. Személyes azonosság hitelesítése „Személyes" tanúsítvány igénylése esetén

A természetes személy Igénylonek (Elofizetonek) a tanúsítványkérelemhez csatolnia kell a Szolgáltató által biztosított regisztrációs urlapot kitöltve és aláírva.

A természetes személy hitelesítéséhez a következo adatokat kéri az Ügyfélkapcsolati Iroda:

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

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

Az Ügyfélkapcsolati Iroda az átadott azonosító-hitelesíto dokumentumok érvényességének és hitelességének biztonságos megállapítása érdekében kiegészíto ellenorzést végezhet a Szolgáltató Biztonsági Szabályzatában szabályozott módon.

Az Elofizeto 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, felelosségét és jogait ismeri, s elfogadja azokat

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

3.1.8. Szervezeti identitás hitelesítése „Szervezeti személy" tanúsítvány igénylése esetén

Az igénylo szervezetnek (Elofizetonek) a tanúsítványkérelemhez csatolnia kell a Szolgáltató által biztosított regisztrációs urlapot kitöltve, és a szervezet képviseletére jogosult vezeto tisztségviseloinek az aláírásával ellátva.

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

a. az igénylo 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 elofizeto 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 cégszeruen aláírva (a dokumentum tartalmazza a megbízó szervezet vagy szervezeti egység nevét, e-mail címét, telefon+fax számát)
h. az elofizeto szervezet egyértelmu hozzájárulása ahhoz, hogy:
  - a tanúsítvány kibocsátásra kerüljön
  - a szervezet vagy szervezeti egysége neve a tanúsítvány tulajdonosazonosító mezojében feltüntetésre kerüljön
  - az Aláíró neve a tanúsítvány tulajdonosazonosító mezojében feltüntetésre kerüljön
  - a Szolgáltató a regisztráció során a szervezeti azonosság hitelesítésére elfogad minosített aláírással ellátott elektronikus okiratot is abban az esetben, ha az Elofizetovel ebben elozetesen megegyezik. Ez esetben az Elofizeto szervezeti azonosságának hitelesítése, s a szervezeti adatok felvétele a megegyezés során történik, az elektronikus okirat „már csak" az Elofizeto hozzájárulását tartalmazza az Aláíró részére történo tanúsítvány kibocsátásához
  - az Elofizeto kapcsolattartókat nevez meg a Szolgáltató részére, akik aláírási joggal rendelkeznek a tanúsítvány kibocsátását illetoen; a Szolgáltató később e személyeknek az aláírását fogadja el bármilyen kérelem vagy bejelentés esetén
  - az Elofizeto 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, felelosségét és jogait ismeri, s elfogadja azokat

A fentieken kívül még a következoket kell megadni:

a. az Aláíró kijelölését engedélyezo személy neve (az engedélyezonek minden esetben a szervezet képviseletére jogosult személynek kell lennie és ezt hiteles dokumentumokkal (pl. aláírási címpéldánnyal) kell igazolni)

b. az engedélyezo személy beosztása

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

Ezen adatokat a következo dokumentumokkal kell hitelesíteni:

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

b. képviseleti megbízás cégszeruen 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 Fovárosi Bíróság, egyéni vállalkozók esetében az illetékes önkormányzat, ügyvédek esetében az Ügyvédi Kamara, könyvvizsgálók esetében a Könyvvizsgálói Kamara, igazságügyi szakértok esetében az Igazságügyi Minisztérium, stb.,

e. állam-, illetve közigazgatási szervezetek esetében az alapító dokumentum közjegyzovel hitelesített másolata, amelyet a szervezet elso számú vezetojének írásos nyilatkozata kísér,

f. aláírási címpéldány, amely a szervezet aláírásra jogosult vezetoinek 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 ellenorzi. Szervezeti személy típusú tanúsítvány igénylés esetén az Ügyfélkapcsolati Iroda az aláírási jogosultság ellenorzése céljából adategyeztetést végezhet a cégnyilvántartással[6].

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

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

b. a bemutatott dokumentumok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel

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

d. a szervezet kiléte nem állapítható meg minden kétséget kizáróan

e. nem egyértelmu a szervezet felhatalmazása a tanúsítvány kibocsátására

3.1.9. Személyi és szervezeti identitás hitelesítése idobélyegzés illetve OCSP szolgáltatás igénylés esetén

Idobélyegzés szolgáltatást igényelhet:

a. természetes személy

b. jogi személy (szervezet)

Az idobélyegzés illetve OCSP szolgáltatás igénybe vétele a Szolgáltató és az Elofizeto között megkötött szolgáltatási szerzodés keretében lehetséges. Ezen szerzodés keretében az Elofizeto írásbeli nyilatkozatot ad arra vonatkozóan, hogy a Szolgáltató nyilvánosan közzétett szabályzataiban részletesen tárgyalt kötelezettségeit, felelosségét és jogait ismeri, s elfogadja azokat.

Az idobélyegzés illetve OCSP szolgáltatás igénybe vételére vonatkozó szerzodés megkötése érdekében az Ügyfélkapcsolati Iroda az elofizeto személy illetve szervezret azonosítása érdekében a 3.1.7 illetve 3.1.8 pontokban leírt azonosítási módokat alkalmazhatja.

Az Ügyfélkapcsolati Iroda az idobélyegzés illetve OCSP szolgáltatási szerzodés megkötése során megtagadhatja a szerzodés megkötését, amennyiben

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

b. a bemutatott dokumentumok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel

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

[6] Eat. 12. § (2) b)

d. a szervezet kiléte nem állapítható meg minden kétséget kizáróan

e. nem egyértelmu a szervezet felhatalmazása a tanúsítvány kibocsátására

Az idobélyegzés szolgáltatás igénybe vételekor a Szolgáltató az igénybe vevonél biztonságos csatornán keresztüli tanúsítvány alapú kliens azonosítást, vagy egyéb, az elofizeto egyértelmu azonosítását lehetové tevo megoldást alkalmaz.

3.2. Érvényes tanúsítvány megújítása (tanúsítvány frissítése)

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

Elofizetoi tanúsítvány megújítása akkor lehetséges, ha:

a. a tanúsítvány nem szerepel a Visszavont Tanúsítványok Listájában

b. a regisztráció alkalmával rögzített összes adat még érvényességérol és változatlanságáról az Elofizeto hitelt érdemlo módon írásban nyilatkozik.

A Szolgáltató az Elofizeto nyilatkozata alapján adatai érvényességérol és változatlanságáról az illetékes hatóságokkal egyeztetést végez.

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

A Szolgáltató a tanúsítvány megújítás szükségességérol a lejárat elott legfeljebb 30 nappal e-mailben értesítést küld az Elofizetonek, illetve az Aláírónak.

3.3. 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.

3.4. Felfüggesztés és visszavonás kérés

A Szolgáltató gondoskodik arról, hogy az általa kibocsátott tanúsítványok érvényességét az Elofizeto vagy az Aláíró kérésére felfüggessze vagy a tanúsítványt visszavonja. Ennek érdekében a Szolgáltató a 4.6 pontban rögzíti a tanúsítványok visszavonásának és felfüggesztésének eljárásait.

4. A muködésre vonatkozó követelmények

4.1. Tanúsítványigénylés

A Szolgáltatónak azt megelozoen, hogy egy Elofizetovel szerzodéses kapcsolatot létesít, tájékoztatnia kell az Elofizetot a tanúsítvány és/vagy az idobélyeg illetve OCSP szolgáltatás használatával kapcsolatos kikötésekrol és feltételekrol a 2.6.1 pontban megadottak szerint.

Tanúsítvány igényléséhez ki kell tölteni a regisztrációs urlapot és le kell folytatni a 3.1.7 vagy a 3.1.8 pontokban meghatározott regisztrációs eljárást. Az urlap igényelheto az Ügyfélkapcsolati Irodánál, vagy letöltheto a Szolgáltatás Internetes honlapjáról.

Az Elofizetoi Szerzodés aláírásával Elofizeto egyúttal nyilatkozik arról is, hogy a Szolgáltató feltételei és kikötései, valamint saját kötelezettségei vonatkozásában tájékoztatást kapott, azokat elfogadja. Az aláírással az Elofizeto hozzájárul a szolgáltatások során felhasznált adatoknak a Szolgáltató által történo nyilvántartásba vételéhez, Tanúsítványa és az azzal kapcsolatos állapot információk szolgáltatói tanúsítványtárban való közzétételéhez, s ezen információ harmadik félhez történo továbbításához a Szolgáltató szolgáltatásainak leállítása esetén, illetve egyéb jogszabályok által meghatározott esetekben. Az Elofizeto 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 késobbi változásairól a Szolgáltatót értesíti

A regisztráció során az Ügyfélkapcsolati Iroda nyilvántartásba vesz minden, az Aláíró azonosítására használt adatot és információt, beleértve az igazoláshoz használt dokumentáció regisztrációs számát és az annak érvényességével kapcsolatos esetleges korlátozásokat. Az Elofizeto tudomásul veszi és elfogadja, hogy a dokumentációkról az Ügyfélkapcsolati Iroda másolatot készíthet.

A Tájékoztató a szolgáltató internetes honlapján bárki számára elérheto.

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 Tanúsítványt a Szolgáltató a következo módon juttatja el az Elofizetohöz:

a. az Elofizeto, az Aláíró vagy azok képviseloje személyesen átveheti az Ügyfélkapcsolati Irodán, vagy
b. postai úton eljuttatja az Elofizeto által megadott címre, vagy
c. az Elofizeto letöltheti a Szolgáltató nyilvános Tanúsítványtárából

4.3. Idobélyegzés

Idobélyegzés szolgáltatás igénylése esetén az Igénylot tájékoztatni kell az idobélyeg használat módjáról, az azzal járó kötelezettségekrol és felelosségrol.

Az Igénylo azonosítását a 3.1 pontban leírt egyszerusített eljárással kell elvégezni.

Az idobélyegzés kérelmek teljesítését a Szolgáltató idobélyegzo egysége automatikusan végzi:

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

Az idobélyegzés szolgáltatás az Elofizeto részére a szerzodéskötést követo 24 órán belül megkezdodik.

Az idobélyegben megadott ido 1 másodpercen belüli pontosságot biztosít. Az idobélyegzo egység órájának pontossága folyamatos ellenorzés alatt áll. Ha ez túllépné a pontossági határt, akkor az ellenorzo program leállítja az idobélyegzés szolgáltatást, és minden további kérésre a hiba kijavításáig hibaüzenetet küld a felhasználók felé. A szolgáltatás akkor indul újra, ha az idoszinkron helyreállt és az egymásodperces pontossági határ teljesül. Az idoszinkron helyreállítását a Szolgáltató húsz percen belül biztosítja.

4.4. OCSP szolgáltatás

OCSP szolgáltatás igénylése esetén az Igénylot tájékoztatni kell a használat módjáról, az azzal járó kötelezettségekrol és felelosségrol.

Az Igénylo azonosítását a 3.1 pontban leírt egyszerusített eljárással kell elvégezni.

Az OCSP kérelmek teljesítését a Szolgáltató OCSP egysége automatikusan végzi:

a. a kérelmet egy olyan, a szolgáltatás igénybe vétele céljából megkötött szerzodésben definiált kommunikációs csatornán keresztül fogadja, amelyen keresztül az OCSP válasz kérot 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 Elofizeto részére a szerzodéskötést követo 24 órán belül megkezdodik.

Az OCSP válaszban megadott ido 1 másodpercen belüli pontosságot biztosít. Az OCSP válaszadó egység órájának pontossága folyamatos ellenorzés alatt áll. Ha az ez túllépné a pontossági határt, akkor az ellenorzo program leállítja az OCSP szolgáltatást, és minden további kérésre a hiba kijavításáig hibaüzenetet küld a felhasználók felé. A szolgáltatás akkor indul újra, ha az idoszinkron helyreállt és az egy másodperces pontossági határ teljesül. Az idoszinkron helyreállítását a Szolgáltató húsz percen belül biztosítja.

4.5. Tanúsítvány elfogadás

A tanúsítvány elfogadása az Elofizeto részérol az átadással történik meg.

Az aláírás-létrehozó adat használatba vétele elott az Elofizetonek kötelessége ellenorizni a Tanúsítványban feltüntetett adatainak helyességét. Amennyiben bármilyen rendellenességet talál, az aláírás-létrehozó adatot nem használhatja fel, hanem azonnal intézkednie kell a tanúsítvány visszavonására.

4.6. Tanúsítvány felfüggesztés és visszavonás

A Szolgáltató a tanúsítványok érvényességének kezelésére mind tanúsítvány visszavonási, mind tanúsítvány felfüggesztési szolgáltatásokat nyújt. A tanúsítvány visszavonása a tanúsítvány állapotát végérvényesen érvénytelenre állítja. Felfüggesztés esetén a tanúsítvány csak rövid, átmeneti idoszakra lesz érvénytelen. A tanúsítvány felfüggesztett állapotban csak ideiglenesen lehet, az engedélyezett idotartam (lásd 4.6.6 pont) után állapotát újra érvényesre kell állítani, vagy a tanúsítványt vissza kell vonni.

A visszavont/felfüggesztett Tanúsítványhoz tartozó aláírás-létrehozó adat (magánkulcs) használatát azonnal meg kell szüntetni, illetve fel kell függeszteni. A visszavont Tanúsítványhoz tartozó aláírás-létrehozó adatot, illetve aláírás-létrehozó eszközt a visszavonást követoen azonnal meg kell semmisíteni. A megsemmisítéséig az aláírás-létrehozó adat, illetve eszköz ugyanolyan felügyeletben részesítendo, mintha a tanúsítvány érvényes lenne.

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

4.6.1. Visszavonáshoz/felfüggesztéshez vezeto körülmények

A Szolgáltató felfüggeszti vagy visszavonja a tanúsítvány érvényességét ha:

a. az Elofizeto vagy az Aláíró ezt kéri

b. megalapozottan feltételezheto, hogy a Tanúsítványban foglalt adatok nem felelnek meg a valóságnak, azok használata jogszerutlen, vagy az aláírás-létrehozó adat nem az Aláíró kizárólagos birtokában van

c. a Szolgáltató és az Elofizeto között a szerzodés megszunt

d. a Nemzeti Hírközlési Hatóság jogeros és végrehajtható határozatában így rendelkezik

e. a Szolgáltató a szolgáltatással kapcsolatos rendellenességrol vesz tudomást és a rendellenesség az érvényes szabályok szerint nem orvosolható

f. a Szolgáltató a tevékenységét befejezte

Az Elofizeto vagy az Aláíró a következo 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 védo aktivizáló adat (PIN kód) kompromittálódása, vagy annak gyanúja

d. a Tanúsítványban feltuntetett hibás adatok

e. az Elofizeto Tanúsítványban feltuntetett adatainak megváltozása
f. az Aláíró Tanúsítványban feltuntetett adatainak megváltozása
g. a Tanúsítványban feltuntetett Aláíró és szervezet kapcsolatának megváltozása vagy megszunése[7].

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

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

a. a tanúsítvány felfüggesztési idejének lejárata
b. amennyiben a törvény erre kötelezi
c. az ÁSZF-M vagy az Elofizetoi Szerzodés megszegése az Elofizeto és/vagy az Aláíró által
d. az Elofizeto és/vagy az Aláíró kötelezettségeinek be nem tartása
e. az Elofizetoi szerzodés megszunése
f. a Szolgáltató tudomására jutott tény, vagy alapos gyanú, a regisztrációs adatok valótlanságáról
g. a Tanúsítványban feltuntetett kibocsátó adatok megváltozása
h. a hitelesítési szolgáltatás megszunése
i. a Szolgáltató valamely magánkulcsának kompromittálódása miatt

A Szolgáltató egy tanúsítvány hitelességével kapcsolatosan felmerülo kétely vagy a hitelesség sérülésének alapos gyanúja esetén dönthet a tanúsítvány felfüggesztésérol. Ilyen esetekben a Szolgáltatónak a felfüggesztett állapot idotartama alatt intézkednie kell a körülmények tisztázása érdekében.

4.6.2. Visszavonás/felfüggesztés kérelmezése

Tanúsítvány visszavonását vagy felfüggesztését az elozo pontban feltüntetett körülmények alapján az Aláíró, az Elofizeto vagy annak a regisztráció során nyilvántartásba vett képviseloje, a Szolgáltató, hatósági szervezet vagy más harmadik fél kezdeményezheti. Az Elofizetonek és Szolgáltatónak kötelessége, harmadik félnek joga, a feltuntetett esetekben a visszavonás azonnali kezdeményezése.

Felfüggesztési kérelmet be lehet nyújtani személyesen vagy írásban a Szolgáltató Ügyfélkapcsolati Irodájánál. A bejelento akadályoztatása vagy azonnali intézkedés szükséges ége esetén a tanúsítvány felfüggesztése telefonon vagy elektronikusan aláírt e-mail-ben is kérheto az Ügyfélszolgálaton. A tanúsítvány visszavonására az ettol számított 30 napon belül lehet intézkedni.

Minosített tanúsítványra a visszavonási kérelmet a Szogáltató csak a következo formában fogadja el:

a. személyesen az Ügyfélkapcsolati Irodánál
b. közjegyzovel hitelesített írásbeli nyilatkozatban
c. az Aláíró által az Ügyfélkapcsolati Irodához címzett, minosített aláírással hitelesített elektronikus dokumentumban.

A visszavonási kérelemnek a következo adatokat kell tartalmazni:

a. a tanúsítvány sorszáma, vagy egyéb olyan adatok, amely alapján a Szolgáltató rendszerében a tanúsítvány egyértelmuen azonosítható
b. a visszavonást kéro megnevezése, azonosító adatai
c. a visszavonást kéro e-mail címe (ha van)
d. a visszavonás hoz vezeto körülmények.

A felfüggesztési kérelemnek a visszavonási kérelemmel megegyezo adatokat (illetve a Szolgáltató ügyfélszolgálatán keresztül történo bejelentés esetén azokon túlmenoen a felfüggesztési jelszót) kell tartalmaznia.

4.6.3. Visszavonási/felfüggesztési kérelemre vonatkozó türelmi ido

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 állapot közzététele között: 30 perc.

A Szolgáltató akkor tekinti a visszavonási/felfüggesztési kérelmet elfogadottnak, ha annak jogosságáról meggyozodött. A visszavonási/felfüggesztési kérelemre vonatkozó türelmi ido 5 munkanap. Ha a Szolgáltató ezen idon belül sem tud a kérelem jogosságáról meggyozodni, akkor a felfüggesztési/visszavonási kérelmet visszautasítja.

Visszavont/felfüggesztett tanúsítványt joghatályosan nem lehet felhasználni.

A Szolgáltatót és az Elofizetot érinto felelosségi szabályok:

[7] Eat. 10. § (3)

a. A visszavonási/felfüggesztési kérelem bejelentésének a Szolgáltatóhoz történo megérkezéséig és elfogadásáig az ÁSZF-M-nek megfeleloen az Elofizeto felelos a felmerülo károkért.

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

c. A Visszavont Tanúsítványok Listájában való megjelenése után az Érintett fél felelos a felmerülo károkért.

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

4.6.4. Visszavonási eljárás

A visszavonási eljárás elso lépéseként a Szolgáltató azonosítja a bejelentot, majd mérlegeli a visszavonási okokat.

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

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

Szolgáltató a visszavonás megtörténtérol vagy visszautasításáról értesíti az Aláírót, az Elofizetot és a visszavonás kérelmezojét.

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

Elofizetoi tanúsítvány visszavonását a Szolgáltató akkor is nyilvánosságra hozza, ha a tanúsítvány közzétételéhez az Elofizeto nem járult hozzá.

4.6.5. Felfüggesztési eljárás

A felfüggesztési eljárás elso lépéseként a Szolgáltató azonosítja a bejelentot, majd mérlegeli a felfüggesztési okokat:

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

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

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

Szolgáltató a felfüggesztés megtörténtérol vagy visszautasításáról értesíti az Aláírót, az Elofizetot és a visszavonás kérelmezojét.

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

Elofizetoi tanúsítvány felfüggesztését a Szolgáltató akkor is nyilvánosságra hozza, ha a tanúsítvány közzétételéhez az Elofizeto nem járult hozzá.

4.6.6. A felfüggesztett állapotra vonatkozó korlátozások

Tanúsítvány felfüggesztett állapotban legfeljebb 5 naptári napig lehet.

Ha a felfüggesztést az Elofizeto vagy az Aláíró kérte, akkor a kérelmezonek ezen idoszak alatt értesítenie kell a Szolgáltatót a tanúsítvány érvényesítése vagy visszavonása felol. Ha ilyen értesítés nem történik Szolgáltató a Tanúsítványt visszavonja.

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

A felfüggesztés megszüntetése a felfüggesztési idoszak vége elott is kérheto. A felfüggesztés megszuntetésének eredménye a tanúsítvány újraérvényesítése vagy visszavonása lehet.

Az újraérvényesítés feltételei a következok:

a. az újraérvényesítést csak az Elofizeto vagy annak a regisztráció során nyilvántartásba vett képviseloje kérheti

b. az újraérvényesítést kéro személyt azonosítani és hitelesíteni kell

Az újraérvényesítés kéréséhez a következo adatokat kell megadni:

a. a felfüggesztett tanúsítvány sorszáma

b. a felfüggesztés megszüntetést kéro azonosító adatai

c. a felfüggesztés megszüntetés kérés oka

4.6.7. Visszavont Tanúsítványok Listája (CRL) és kibocsátásának gyakorisága

A Visszavont Tanúsítványok Listájában a visszavont és felfüggesztett tanúsítványok kerülnek feltüntetésre. A felfüggesztett tanúsítványok az újraérvényesítés hatására kerülhetnek ki a listából. Szolgáltató fenntartja a jogát arra vonatkozóan, hogy a lejárt Tanúsítványokat kitörölje a listából.

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

A Szolgáltató egy-egy tanúsítvány felfüggesztését, visszavonását illetve újraérvényesítését követoen haladéktalanul új visszavonási listát tesz közzé.

4.6.8. Visszavont Tanúsítványok Listája ellenorzési követelmények

A Visszavont Tanúsítványok Listája ellenorzése az érintett felek felelossége a tanúsítványok elfogadását megelozoen. A Tanúsítványhoz tartozó visszavonási lista elérhetoségét a tanúsítvány tartalmazza. A lista ellenorzésének arra kell vonatkozni, hogy a kérdéses Tanúsítványt a lista tartalmazza-e (és ha igen, milyen idoponttól), a lista hiteles és sértetlen, s a kérdéses tranzakció szempontjából idoben releváns-e.

A tanúsítvány visszavonási listában a Szolgáltató által közzétett érvénytelen, vagy felfüggesztett tanúsítvány elfogadásából keletkezo bárminemu kár Érintett felet terheli.

4.6.9. Visszavonási állapot közlés más formái

A Szolgáltató a Visszavont Tanúsítványok Listája mellett online visszavonási információs (OCSP) szolgáltatást nyújt. Az OCSP szolgáltatás nyújtása elsosorban a 4.4 és 3.1.9 pontokban foglaltaknak megfeleloen történik.

4.6.10. Magánkulcs kompromittálódás speciális követelményei

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

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

4.7. Biztonsági audit eljárások

A Szolgáltató hitelesítés-szolgáltatását és idobélyegzését támogató informatikai rendszerének biztonsági naplózását és annak auditálását a jelen HSZSZ-M mellett a biztonsági szabályzat szabályozza részletesen.

4.7.1. Naplózott esemény típusok

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

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

a. a szolgáltatói tanúsítványok életciklusával kapcsolatos összes eseményt

b. az elofizetoi tanúsítványokat aláíró infrastruktúrális és ellenorzo kulcsok tanúsítványainak életciklusával kapcsolatos összes eseményt, ezen belül különösen az elofizetoi tanúsítványok eloállítási és megújítási igény-benyújtási idopontját, valamint az igények teljesítésének idopontját

Az Elofizetok 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 eloállt tevékenységek naplózásáról.

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

a. az idobélyegzés szolgáltatás fo lépései, a kérelemtol az idobélyeg válasz elküldésig

b. az idobélyeget aláíró kulcs ok életciklusában bekövetkezo eseményeket (generálás, használat, visszavonás, megsemmisítés)

c. az idobélyeget aláíró kulcs ok tanúsítványa életciklusában bekövetkezo eseményeket (kiadás, has ználat, visszavonás)

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

a. az OCSP szolgáltatás fo lépései, a kérelemtol az OCSP válasz elküldésig

b. az OCSP válaszokat aláíró kulcsok életciklusában bekövetkezo eseményeket (generálás, használat, visszavonás, megsemmisítés)

c. az OCSP válasz aláíró kulcsok tanúsítványa életciklusában bekövetkezo eseményeket (kiadás, has ználat, 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 történo bármely hozzáférési kísérlettel kapcsolatos eseményeket

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

A pontos idot a Szolgáltató idobélyegzo egysége biztosítja.

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

4.7.2. Napló adatok védelme

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

A Szolgáltató biztosítja naplóállományok bizalmasságát és sértetlenségét.

4.7.3. Napló adatok feldolgozása

A PKI alkalmazás, az idobélyegzés alkalmazás és az operációs rendszerek biztonsági esemény és audit naplóinak operatív ellenorzését csak a rendszervizsgálók végezhetik és csak olvasási jogosultsággal. A rendszervizsgálók feladata az alkalmazásokon és operációs rendszereken kívüli, de a PKI rendszer részét képzo szoftver elemek (hálózat, tuzfalak, betörés detektor) naplóinak ellenorzése is.

4.7.4. Napló adatok tárolása

A napló adatokat a Szolgáltató archiválja (lásd: 4.8.3 pont).

4.7.5. Rendkívüli eseményekrol történo értesítés

A szolgáltatás támogató informatikai rendszerre, annak fizikai és személyi környezetére kiható súlyos üzemzavari és katasztrófa események megelozéséről, kezeléséről, az érintettek értesítéséről és a rendszer visszaállításáról részletesen a Szolgáltató Üzletmenet-folytonossági Terve intézkedik. Az Üzletmenet-folytonossági Tervben az üzletmenetet veszélyezteto, sérto, illetve azt leállító események súlyossági osztályokba vannak sorolva. A Terv részletesen szabályozza a Hitelesíto Központok saját aláírás-létrehozó adatainak, aktiváló adatainak és az idobélyegek aláíró kulcsának kompromittálódása esetén elvégzendo teendoket.

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

4.8. Adatarchiválás

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

4.8.1. A tárolt adatok típusai

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

a. az Igénylo által a regisztráció támogatása céljából benyújtott dokumentum(ok) típusa
b. az azonosító dokumentumok egyedi azonosító adatai (például az Igénylo jogosítvány száma)
c. az Igénylo és azonosító dokumentumok (beleértve az aláírt, az Elofizetovel kötött megállapodást másolatainak tárolási helyszíne)
d. az Elofizetovel kötött megállapodás esetleges egyedi választásai
e. a kérelmet elfogadó regisztrációs felügyelo (RO) azonosítója
f. a fogadó Hitelesíto Központ és/vagy a küldo regisztrációs felügyelo (RO) azonosítója, amennyiben ez értelmezheto

A 4.7.1 pontban felsorolt összes esemény, illetve napló típus.

4.8.2. Az archívum gyujtési rendszere

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

4.8.3. Az archívum megorzési idotartama

A Szolgáltató 4.8.1 pontban megnevezett nyilvántartásokat és a 4.7.1 pontban megnevezett naplókat a 3/2005. (II. 18) IHM rendelettel összhangban a keletkezésüktol számított 10 évig, illetve jogi eljárásban a tanúsítványokon keresztül történo bizonyításhoz szükséges ideig megorzi.

4.8.4. Az archívum védelme

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

4.8.5. Az archívum hozzáférését és ellenorzését végzo eljárások

A Szolgáltató az archívumhoz Ügyfélkapcsolati Irodáján keresztül biztosít hozzáférést és értelmezhetoséget. A jogosultságot és a hozzáférést a Szolgáltató a minden esetben ellenorzi és naplózza.

4.9. A folyamatos üzemmenet biztosítása (katasztrófa elhárítás)

A Szolgáltató olyan megbízható rendszert muködtet, amely a rendszerben bekövetkezett hiba esetén is biztosítják a szolgáltatások elérhetoségét.

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 leheto legrövidebb idon belül helyreálljon.

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

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

A rendkívüli üzemeltetési helyzetekben a Szolgáltató eseménynaplótvezet.

4.9.1. Biztonsági képesség rendkívüli üzemeltetési helyzetben

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

A visszaállítási idot alapvetoen az esemény súlyossága, azaz az Üzletmenet-folytonossági Terv szerint értelmezett osztályba sorolása határozza meg. A súlyos üzemzavari és a katasztrófa esetet – többek között – az különbözteti meg, hogy katasztrófa esetén nagy valószínuséggel nem csak az informatikai rendszer, hanem annak fizikai környezete is megsemmisül részben vagy egészben. Ez utóbbi esetben az Üzletmenet-folytonossági Tervben meghatározott módon a Válság Stáb intézkedik a katasztrófa (tartalék) helyszínre történo áttelepülésrol és az informatikai rendszer részleges vagy teljes visszaállításáról a katasztrófa helyszínen korábban elhelyezett mentések segítségével.

4.9.2. Minimális szolgáltatás rendkívüli üzemeltetési helyzetben

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

Minden egyéb szolgáltatást a Szolgáltató szüneteltet.

A normális üzemmenet helyreállítására vonatkozó eljárásokat a Szolgáltató üzletmenet-folytonossági terve tartalmazza.

4.9.3. 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.

4.10. A hitelesítés-szolgáltatási tevékenység megszüntetése

A Szolgáltató a tervezett megszunés elott tárgyalásokat kezd más szolgáltatókkal a szolgáltatások átvételérol. A tárgyalások eredményérol tájékoztatja a felhasználói közösséget.

A Szolgáltató gondoskodik a szolgáltatásainak megszüntetésébol fakadó, a felhasználói közösséget érinto zavarok minimalizálásáról. Különösképpen gondoskodik a tanúsítvány visszavonás kezelés és közzététel szolgáltatások folyamatos fenntartásáról.

Ennek érdekében a Szolgáltató mielott hitelesítés-szolgáltatási tevékenységét leállítja:

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

b. megszunteti 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 egyidejuleg a Szolgáltató leállítja:

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

b. az Idobélyegzés és OCSP szolgáltatást

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

Szolgáltató a tervezett megszunés elott 20 nappal intézkedik az elofizetoi tanúsítványok és saját felhasználású tanúsítványok visszavonásáról.

Ezzel egyidejuleg leállítja a visszavonás kezelési szolgáltatást.

Szolgáltató nem biztosít a szokásosnál és a jogszabályokban eloírtnál nagyobb mértéku adatszolgáltatást a megszunéskor.

Eljárás Regisztrációs Iroda megszunése esetén:

a. A Regisztrációs Iroda megszunése elott 60 nappal értesíti azon Elofizetoket, akik a megszuno Regisztrációs Irodától kapott, a Szolgáltató által kibocsátott érvényes tanúsítvánnyal rendelkeznek.

b. A Regisztrációs Iroda megszunésérol a felhasználói közösség tagjait Szolgáltató a web oldalain történo közzététel útján tájékoztatja.

5. Fizikai, eljárásrendi, és humán biztonsági szabályozások

A Szolgáltató elismert szabványoknak megfelelo fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket és az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmaz. Ezen belül:

a. A Szolgáltató kockázat elemzést végzett üzleti kockázatainak felmérése, valamint a szükséges biztonsági követelmények és muködési eljárások meghatározása érdekében

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

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

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

A Szolgáltató biztonsági muveletei közé az alábbiak tartoznak:

a. üzemeltetési eljárások és felelosségek
b. ellenorzési eljárások
c. biztonsági rendszerek és eljárások tervezése, elfogadása és muködtetése
d. eroforrás gazdálkodás
e. hálózat menedzselés
f. a biztonsági naplók aktív felügyelete, eseményelemzések és nyomkövetések
g. adathordozó eszközök kezelése és biztonsága
h. rendszerkarbantartás

E felelosségeket a Szolgáltató biztonsági muveletei kezelik, és azokat a 3/2005. (III. 18) IHM rendeletnek megfelelo, megbízható és szakérto üzemelteto személyzet hajthatja végre.

A Szolgáltató gondoskodik arról, hogy eszközei és információi megfelelo szintu védelemben részesüljenek. A Szolgáltató valamennyi informatikai értékérol leltárt vezet, ezek védelmi követelményeit osztályokba sorolja és minosíti, az elvégzett kockázat elemzéssel összhangban.

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

A szolgáltatást támogató informatikai rendszer, annak személyi és fizikai környezete a MeH ITB 12. ajánlás szerint a fokozott biztonsági osztályba tartozik, amely egyértelmuen meghatározza a Hitelesíto Központok, az idobélyegzo egységek és a Regisztrációs Iroda informatikai rendszereinek, személyi és fizikai környezetének biztonsági követelményeit.

A következo pontok csak a vonatkozó lényeges intézkedéseket tartalmazzák.

5.1. Fizikai biztonsági szabályozások

5.1.1. Hitelesíto Központok

A hitelesíto központok és idobélyegzo egységek legmagasabb védelmi szintet képezo objektuma a Bizalmi Központ, amely a biztonsági szempontból legkritikusabb hardver/szoftver modulokat tartalmazza. Ez az objektum kielégíti a MeH ITB 12. ajánlás szerinti fokozott biztonsági osztály fizikai védelmi követelményeit A Bizalmi Központ:

a. a fokozott biztonsági szintnek megfelelo szilárdságú határoló felületekkel határolt, ajtói rendelkeznek MABISZ minosítésse rendelkeznek, nyitásukra kulcskezelés szabályozás érvényes

b. elotte biztonsági szegmens van kialakítva, amelybe anti-passback és naplózási tulajdonságokkal bíró belépteto rendszeren keresztül lehet csak bejutni. A bejutást video biztonsági kamerás rendszer figyeli, amelynek személyes felügyelete folyamatosan biztosított,

c. rendelkezik önálló és kettozött klimatizálással, mozgásérzékelo, tuz-, víz- és füstjelzo és tuzoltó rendszerrel, szünetmentes tápáramellátó rendszerrel, az MSZ 274/5T:1993 szabvánnyal összhangban LPZ2 zónahatárig kiépített másodlagos villámvédelemmel valamint 60 DB elnyomással rendelkezo EMC védelemmel

d. a Bizalmi Központban a szerverek biztonsági kabinetekben vannak elhelyezve

e. a Bizalmi Központba csak a Biztonsági Szabályzatban meghatározott szerepköru vezetok és munkatársak léphetnek be meghatározott céllal,

f. a mentési és a primer szoftver adathordozók, a nyers- és a megszemélyesített láírás-létrehozó eszközök besugárzás és fizikai behatás ellenálló biztonsági szekrényekben vannak tárolva

g. az informatikai rendszer két független nyomvonalon vezetett üvegkábellel kapcsolódik az Internethez,

h. a lokális telefonkapcsolat az EMC zónahatáron szuron keresztül kapcsolódik a szolgáltató telefonközpontjához.

A környezetei elemek, rendszerek állapotjellemzoit monitor rendszer figyeli. A bekövetkezo események naplózásra, majd archiválásra kerülnek.

5.1.2. Regisztrációs Iroda

A regisztrációs iroda a Bizalmi Központon belül van kialakítva, itt találhatók a regisztrációs munkahelyek és munkaállomások.

5.2. Eljárásrendi szabályozások

A Szolgáltató eljárásrendi szabályait a következo szabályzatok tartalmazzák:

a. a Szervezeti és Muködési Szabályzat, amely részletesen meghatározza a Szolgáltató szervezeti felépítését, azon belül az egyes munkaköröket és az azokhoz kapcsolt feladat-, felelosség és hatásköröket,

b. a jelen HSZSZ-M,

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

5.2.1. Bizalmi munkakörök

Jelen pont 1. táblázatában a hitelesítés- és Idobélyegzés és OCSP szolgáltatásokhoz kapcsolódó szerepkörök, azok feladat-, felelosség és hatáskörei kerülnek összefoglalásra.

Szerepkör	Feladatkör	Felelosségi kör	Hatáskör
A Szolgáltató vezetoje	A Szolgáltató szervezet irányítása és ellenorzése	Folyamatos és biztonságos szolgáltatás. A PKI Rendszer és adat tulajdonosa	A Szolgáltató munkáltatói jogköre. A teljes szervezet szintjén dönt
A PKI Szolgáltató Egység vezetoje	A Szolgáltató szervezet szolgáltatási tevékenységének irányítása és ellenorzése	Folyamatos és biztonságos szolgáltatás. PKI Rendszer muködtetésének egy-személyi felelos vezetoje	A Szolgáltató szervezet szintjén dönt, intézkedik.
Ügyfélkapcsolati Iroda vezetoje	Az ügyfélkapcsolati tevékenység irányítása és ellenorzése.	Az ügyfelek biztonságos azonosítása-hitelesítésének ellenorzése.	Az ügyfélkapcsolati tevékenység ellenorzése.
Hitelesítés Pol. és Szab. Csop. Vezeto	Politikák, szabályzatok kialakítása, PKI belso ellenorzés	Politikák, szabályzatok és gyakorlat összhangja	Politikák, szabályzatok érvényesítése, PKI belso audit
A Szolgáltató IB vezetoje	IB tevékenység irányítása, ellenorzése a Szolgáltató minden területén.	IB kockázatok elviselheto szinten tartása	IB intézkedések, IB belso ellenorzés.
Üzemeltetés vezeto	Az IT rendszer üzemeltetés irányítása	Az üzemeltetés folyamatossága, minosége, biztonsága	Intézkedés az IT rendszer minden szintjén üzemeltetési kérdésekben
Üzemelteto adminisztrátor	Üzemeltetési adminisztráció, hibaelhárítás, karbantartás	Az üzemeltetés folyamatossága, minosége	Operatív intézkedés az üzemeltetés területén
IB adminisztrátor	Biztonsági beállítások, adminisztráció, karbantar-	Az üzemeltetés biztonsága	Operatív ellenorzés, operatív intézkedés

Szerepkör	Feladatkör	Felelosségi kör	Hatáskör
	tás		
Hitelesíto biztonsági felügyelo (Security Officer /SO/)	RO kulcsok, tanúsítványok létrehozása	Saját kulcs, PKI és Idobélyegzés és OCSP alkalmazás és adatok biztonsága	RO és ügyfél kulcsok, tanúsítványok létrehozása.
Regisztrációs felügyelo (Registration Officer /RO/)	Regisztrációs Iroda irányítása. Elofizeto regisztráció, kulcs, tanúsítvány igénylése, kulcs megszemélyesítése	Regisztrációs Iroda folyamatos muködtetése.	Regisztrációs Irodán intézkedési jog. SO hatásköre nem lehet.
Rendszer operátor	Üzemeltetési rutin tevékenységek PKI szinten.	A PKI és Idobélyegzés és OCSP alkalmazás üzemeltetésének folyamatossága,	Rutin operátori tevékenység az Üzemeltetési Kézikönyv szerint
Rendszer vizsgáló (auditor)	Operatív funkcionális és biztonsági ellenorzések.	Funkcionális és biztonsági hiányosságok, visszaélések felfedése.	Biztonsági és audit naplók ellenorzése.

1. táblázat

5.2.2. Az egyes feladatokhoz szükséges személyzeti létszámok

Minden rendszer-telepítési, hardver-beavatkozást és szoftver-frissítést igénylo beavatkozást két munkatárs egyideju jelenlétében lehet elvégezni. A muveletek sikerességét auditoroknak kell ellenorizni és hitelesíteni.

Továbbá két SO együttesen végezheti az alábbi feladatokat:

a. a PKI alkalmazás installásához szükséges szolgáltatói kulcspárok generálása a Szolgáltató vezetoje által kijelölt bizottság jelenlétében

b. a hitelesíto központok szolgáltatói tanúsítványaihoz tartozó kulcspárjainak generálása a Szolgáltató vezetoje által kijelölt bizottság jelenlétében

c. a szolgáltatói magánkulcsok biztonsági mentése

d. a szolgáltatói magánkulcsok mentésbol történo visszaállítása

e. a szolgáltatói magánkulcsok (és másodpéldányainak) megsemmisítése

f. a szolgáltatói nyilvános kulcsokat tartalmazó token Root CA-hoz való továbbítása, illetve a Root CA által kibocsátott tanúsítványok visszaszállítása a Szolgáltató vezetoje által kijelölt bizottság jelenlétében

g. a Root CA nyilvános kulcsát tartalmazó tokennek a Produktív CA-hoz való továbbítása a Szolgáltató vezetoje által kijelölt bizottság jelenlétében

h. az RO szolgáltatói kulcspárok generálása, cseréje és megsemmisítése.

5.2.3. A bizalmi munkakörökben elvárt azonosítás és hitelesítés

A PKI alkalmazásokba történo belépéshez a bizalmi munkakört betölto munkatársak azonosítása és hitelesítése egy szolgáltatói tanúsítvánnyal rendelkezo csipkártya kártyaolvasóba helyezésével, majd az azt aktivizáló PIN kód megadásával történik.

Sikeres hitelesítés elott egyetlen biztonság kritikus tevékenységet sem lehet végrehajtani.

5.3. Humán szabályozások

A Szolgáltató gondoskodik arról, hogy személyzeti gyakorlata fokozza és támogassa a Szolgáltató muködésének megbízhatóságát, így valamennyi bizalmi munkakört betölto munkatársa független minden olyan ütközo érdektol, ami hátrányosan érinthetné a Szolgáltató tevékenységeinek semlegességét.A munkatársak a feladatok szétválasztása és a legkisebb meghatalmazás szempontjai szerint meghatározott munkaleírásokkal rendelkeznek.. A munkaleírások meghatározzák az egyes feladatokhoz szükséges létszámot is.

5.3.1. Képzettségre, gyakorlatra és biztonsági ellenorzésre vonatkozó követelmények

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

A Szolgáltató kello számú, megfelelo képzettséggel, szakmai ismerettel és tapasztalattal rendelkezo személyzetet alkalmaz.

A vezeto személyzet tapasztalattal rendelkezik az elektronikus aláírási és az Idobélyegzés és OCSP szolgáltatási technológia terén, ismeri a biztonsági felelosséggel tartozó munkatársakra vonatkozó biztonsági eljárásokat, valamint gyakorlattal rendelkezik az informatika biztonság és a kockázat elemzés területein.

5.3.2. Biztonsági háttér ellenorzésekre vonatkozó eljárások

Az alább meghatározott szerepkörök betöltését az átlagosnál magasabb szintu biztonsági ellenorzés elozi meg:

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

A munkakörök betöltéséhez szükséges képzettség és gyakorlat:

biztonsági tisztviselo (IB adminisztrátor, SO):

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

regisztrációs biztonsági tisztviselo (RO):

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

muködteto adminisztrátor, rendszer auditor:

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

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

A szerepkörhöz történo hozzárendeléskor:

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

Kilépéskor:

a. A kilépésrol szóló döntés meghozatalakor a kilépo fizikai és logikai belépési és hozzáférési jogosultságait azonnal meg kell szüntetni. A kilépo ezután az informatikai biztonsági menedzser kíséretében léphet be még egyszer a munkahelyi környezetébe, a személyes dolgai elvitele céljából.
b. A kilépo személy számítógépes tevékenységét legalább két hétre visszamenolegesen le kell ellenorizni.
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 kiléponél levo dokumentációt és ügyiratot vissza kell venni, különös tekintettel a biztonsági és/vagy minosített adatokat információkat tartalmazó anyagokra.
A visszaadott anyagokról tételes átvételi jegyzokönyvet kell felvenni.

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

5.3.3. Képzési követelmények

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

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

Rendszerüzemeltetoi munkakörben kinevezett munkatárs a kinevezést követo 3 hónapig, megfelelo gyakorlattal rendelkezo kollégával közösen van beosztva.

5.3.4. Továbbképzési gyakoriságok és követelmények

Abban az esetben, amikor a szolgáltatásban jelentos változás[8] következik be, valamennyi munkatárs, az ot érinto mélységben továbbképzésben részesül, illetve megkapja a számára szükséges dokumentációkat.[9]

Kisebb változások[10] bekövetkezése elott a munkatársak írásos tájékoztatást kapnak a változásokról.

5.3.5. A felhatalmazás nélküli tevékenységek bünteto következményei

Valamennyi bizalmi munkakört betölto munkatárs a munkaköri kinevezéssel:

a. írásos tájékoztatást kap jogszabályi kötelezettségeirol, jogairól, a személyes adatai kezelésére vonatkozó minosítési és kezelési szabályokról

b. munkaköri leírás a tartalmazza az ot érinto biztonsági feladatokat

c. titoktartási nyilatkozatot ír alá

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

5.3.6. A szerzodéses alkalmazottakra vonatkozó követelmények

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

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

Valamennyi szerzodo fél titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a munkavégzés során birtokába kerülo 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.

5.3.7. A személyzet számára biztosított dokumentációk

A személyzet számára biztosítandó dokumentációt a 9.1 pont sorolja fel.

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

[9] Attól függoen, hogy a bekövetkezo jelentos változás elore tervezett volt, vagy váratlanul kellett sort keríteni rá, a továbbképzés illeszkedik az éves továbbképzési tervekbe, vagy rendkívüli módon, soron kívül iktatódik be.

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

6. Muszaki biztonsági óvintézkedések

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

A rendszert szállítója hitelesítés és Idobélyegzés és OCSP szolgáltatási rendszer kiépítésében jelentos tapasztalatokkal rendelkezik, nemzetközileg elismert technológiát alkalmaz.

6.1. Kriptográfiai kulcspár eloállítás és aláírás-létrehozó eszköz megszemélyesítés

6.1.1. Kulcspár eloállítás

A Szolgáltató maga generálja a szolgáltatói kriptográfiai kulcspárokat (az aláírás-létrehozó és az aláírás-ellenorzo adatot) fizikailag védett környezetben, nagy biztonságú hardver modulban (HSM[11]), kettos ellenorzés mellett. A nagy biztonságú hardver modul hazai tanúsítvánnyal rendelkezik és szerepel a Nemzeti Hírközlési Hatóság által jóváhagyott minosített elektronikus aláírási termék listában. A kulcspár generálást olyan algoritmussal végzi, melyet jogszabály ismer el erre a célra alkalmasnak.

A Szolgáltató nem fogad el az Elofizeto által generált kulcspárt.

Az aláírás-létrehozó adat chip kártyán történo elhelyezésére a Szolgáltató csak tanúsítvány kibocsátással együtt vállalkozik. Ezzel együtt a kibocsátott Tanúsítványt a chip kártyán elhelyezi.

Biztonságos aláírás-létrehozó eszköz alkalmazása esetén (MTT+BALE hitelesítési rend) a kriptográfiai kulcspárt a Szolgáltató PKI alkalmazás a magán a biztonságos aláírás-létrehozó eszközön generálja. Aláírás-létrehozó eszköz alkalmazása esetén (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 idobélyeget illetve az OCSP választ aláíró szolgáltatói kulcsot az idobélyegzo egység szerves részét képezo, tanúsított HSM modul generálja és tárolja. Az aláíró kulcs teljes életciklusa alatt ezen eszközben marad.

6.1.2. Aláírás-létrehozó eszköz megszemélyesítés

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

A chip kártya megszemélyesítés szolgáltatáshoz vizuális megjelenítés, egy oldali nyomással történo grafikus megszemélyesítés is kapcsolódik az Elofizetoi Szerzodésben meghatározott adattartalommal.

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

6.1.3. Az aláírás-létrehozó adat felhasználóhoz történo eljuttatása

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.

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

Az aláírás-létrehozó eszköz átvételének megtagadása visszavonási kérelemnek számít.

6.1.4. Az Aláírók aláírás-ellenorzo adatának eljuttatása a felhasználókhoz

A Szolgáltató az Aláírók aláírás-ellenorzo adatát (nyilvános kulcsát) Tanúsítványtárában teszi mindenki számára elérhetové. Az Aláírók aláírás-ellenorzo adata az Elofizetoi Tanúsítványba van foglalva.

6.1.5. A Szolgáltató aláírás-ellenorzo adatainak eljuttatása a felhasználókhoz

A Szolgáltató a hitelesíto központok (Root CA, Produktív CA) és az idobélyegzo egység aláírás-ellenorzo adatait (nyilvános kulcsait) Tanúsítványtárában teszi mindenki számára elérhetové.

[11] Hardware Security Module

A Tanúsítványtárban közzétett tanúsítványok ellenorzéséhez szükséges nyilvános kulcsok a Szolgáltató Internetes honlapján keresztül közvetlenül is elérhetok.

A tanúsítványok letölthetok és a felhasználó kliens-alkalmazásába installálhatók.

6.1.6. Kulcs méretek

Az Elsodleges (1. szintu) Hitelesíto Központ ("Root CA") aláíró kulcsának mérete:	2048 bit
kommunikációs kulcsának mérete:	1024 bit
A 2. szintu Hitelesíto Központ („Produktív CA”) aláíró kulcsának mérete:	2048 bit
kommunikációs kulcsának mérete:	1024 bit
A Regisztrációs Iroda kommunikációs kulcsának mérete:	1024 bit
Az idobélyegzo egység aláíró kulcsának mérete:	2048 bit
Az Aláírók aláíró kulcsainak (aláírás-létrehozó adatának) mérete:	legalább 1024 bit

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

6.1.7. Elofizetoi aláírás-ellenorzo adat eloállításához használt paraméterek eloállítása

A hitelesíto központ elektronikus aláírásra az RSA[12] algoritmust használják.

Az elofizetoi tanúsítványok az RSA aláíró algoritmusokhoz használhatók.

Az Elofizetoi aláírás-ellenorzo adat eloállításához használt paraméterek megfeleloségét a hazai tanúsító szervezet és a gyártó tanúsítják. A kapcsolódó dokumentumok a Szolgáltatónál megtekinthetok.

6.1.8. Szolgáltatói kulcsgenerálás

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

A produktív hitelesíto központok és az idobélyeget aláíró kulcsok tanúsítványait a Szolgáltató 1. szintu hitelesíto központja (Root CA-ja) hitelesíti.

6.1.9. Kulcs felhasználási célok

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

Az Elofizetok részére kibocsátott tanúsítványok bovítmény (Extension) részében található „KeyUsage” mezobe elektronikus aláírás felhasználási célként a „nonRepudiation” kulcshasználati módnak megfelelo kijelölést kell alkalmazni.

A Szolgáltató Üzleti Egység szervezeti egységei esetében a „Key Usage” mezok lehetséges (egyúttal kötelezoen kitöltendo) értékeit a következo táblázatok mutatják.

Hitelesíto Központ

Kulcs megnevezése	„Key Usage” mezo értéke	Kritikus/Nem kritikus
Hitelesíto Központ (CA) aláíró kulcsa	KeyCertSign, cRLSign	**K**
Idobélyegzo egység aláíró kulcsa	nonRepudiaton	**K**
	Az „Extended Key Usage” mezobe: timeStamping	**K**
A CA PKIX kommunikációs kulcs (Regisztrációs Irodával való biztonságos kommunikáció megteremtésére)	DigitalSign, DataEncipherment, KeyEncipherment	**K**

Regisztrációs Iroda

12 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.

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

6.2. Aláírás-létrehozó adat védelme

6.2.1. A HSM-re vonatkozó szabványok

Az Elofizetok aláírás-létrehozó adatának eloállítására 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.

6.2.2. A több-szereplos (“n-bol m”) magánkulcs visszaállítás ellenorzése

A Szolgáltatónál egyedül a Hitelesíto Központban alkalmazzák az „n-bol m” ellenorzést a Root CA kulcsgondozási funkcióinak aktivizálásánál.

6.2.3. Aláírás-létrehozó adat letét

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

6.2.4. Aláírás-létrehozó adat mentése, duplikálása

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

A Szolgáltatónál a Hitelesíto Központ aláíró magánkulcsai[13] biztonsági okokból duplikálásra kerülnek. A mentés titkosított formában, speciális eszközök alkalmazásával történik.

6.2.5. Aláírás-létrehozó adat kriptográfiai modulba helyezése

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

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

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

6.2.6. Aláírás-létrehozó adat aktiválása

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

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

A szolgáltatói aláírás-létrehozó adatok megsemmisítése a Szolgáltató kötelessége.

6.3. Kulcspár kezelés egyéb aspektusai

6.3.1. Aláírás-ellenorzo adat archiválása

Az aláírás-ellenorzo adatokat a tanúsítványok tartalmazzák. A Szolgáltató minden általa eloállított és kibocsátott Tanúsítványt archivál az alábbi idoszakra:

szolgáltatói tanúsítványokat az érvényesség lejártától számított 10 évig

elofizetoi tanúsítványokat az érvényesség lejártától számított 1 évig

Az archiválás biztonsági okokból 2 példányban történik.

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

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

Root CA aláíró kulcs és tanúsítvány érvényessége:	10 év
Idobélyegzo egység aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 10 év
OCSP válasz egység aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 10 év
Produktív CA aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 10 év
RO kommunikációs kulcs és tanúsítvány érvényessége:	legfeljebb 3 év
Elofizetoi aláíró kulcs és tanúsítvány érvényessége:	1 év

A tanúsítványok és a benne foglalt aláírás-ellenorzo adatok (nyilvános kulcsok) érvényességének kezdete a kibocsátás idopontjával 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 elo.

6.4.2. Aktiválási adatok védelme

A Szolgáltató az Aláíró hozzáférési jogosultságát ellenorzo adatot (PIN-kódot) csak abból a célból rögzítheti, hogy azt az Aláíró számára - másolat megorzése nélkül - átadhassa[14].

A Szolgáltató az aláírás-létrehozó eszközök PIN kódjait muszaki és szervezési intézkedésekkel védi az Elofizetonek vagy az Aláírónak történo átadásig.

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

Az Elofizeto a későbbiekben is bármikor megváltoztathatja a PIN kódját.

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

Az Elofizeto aláírás-létrehozó adatának aktiválási adatát a Szolgáltató az aláírás-létrehozó adat eloállítása után megsemmisíti, büntetojogi felelossége mellett nem hozza harmadik fél tudomására.

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

[14] 3/2005. (III. 18.) IHM rendelet 40. §, 4. bek. szerint.

6.4.3. Aktiválási adatok egyéb aspektusai

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

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

6.5. Számítógép biztonsági szabályok

6.5.1. 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, Idobélyegzés és OCSP alkalmazás,
c. kriptográfiai hardver modulok,
d. tuzfalak, 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 ellenorzés megkerülhetetlenségének biztosítása).

A PKI alkalmazás által megvalósított biztonsági funkciók az alábbiak:

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

Az idobélyegzésre és OCSP szolgáltatásra vonatkozó biztonsági funkciók az alábbiak:

a. Az idobélyeget ileltve OCSP választ aláíró kulcsok tárolása a tanúsítással rendelkezo HSM egység(ek)ben történik. Az idobélyegzo illetve OCSP szerverek külön biztonsági zónában történo üzemeltetése.
b. Az idobélyegzo és OCSP szerverek belso órájának pontossága folyamatos ellenorzés alatt áll. A pontossági tartományból történo kilépés esetén az idobélyegzo illetve OCSP szolgáltatás leáll és a hiba kijavításáig minden további kérésre hibaüzenet kerül kiküldésre.
c. A szinkronizáló órajelek hitelességét az idobélyegzo illetve OCSP informatikai rendszer indításakor egy erre a célra létrehozott bizottság tanúsította. A bizottság minden olyan esetben összehívásra kerül, amikor újrahitelesítés szükséges.
d. biztonsági naplózás,
e. Az idobélyeget illetve OCSP választ kibocsátó szervereket többszörös tuzfal rendszer védi a külso hálózatokról érkezo fenyegetésektol.
f. Az Idobélyegzés és OCSP szolgáltatás rendelkezésre állási szintje 99,9%. Ez a szint meleg tartalékolt idobélyegzo illetve OCSP szerver architektúrával, és a szervereknek a hitelesítés szolgáltató informatikai rendszer magas rendelkezésre állást felügyelo és vezérlo rendszerébe történo 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 ellenorzési szabályok érvényre juttatása),
d. azonosítás és hitelesítés,
e. biztonságkezelés (a hozzáférési jogosultságok szerepkörök szerinti beállítása, módosítása),

f. a biztonsági funkciók megbízható védelme (a hozzáférés ellenorzés megkerülhetetlenségének biztosítása),

g. megbízható út/csatorna (megbízható útvonal kiépítése a magát hitelesíto felhasználóval, mely alkalmas az átvitt adatok illetéktelen felfedésének és módosításának megakadályozására).

A tuzfal 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 ellenorzési szabályok érvényre juttatása/szurés, a tiltott információ áramlás megakadályozása, megfigyelése),

c. azonosítás és hitelesítés,

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

6.5.2. Számítógép biztonsági értékelések

A számítógép biztonsági értékelések rendszerét a 2. táblázat mutatja.

BIZTONSÁGI ELLENORZÉS TÍPUSA		VÉGZI	RENDSZERESSÉG
Operatív	IT infrastruktúra	Informatikai biztonsági adminisztrátor	Naponta
	PKI alkalmazás	Rendszer auditor	Naponta
Belso ellenorzés	IT infrastruktúra	Informatikai biztonsági menedzser	Félévente egyszer
	PKI alkalmazás	Hitelesítési Politika és Szabályozási Csoport	Félévente egyszer
Külso ellenorzés	IT infrastruktúra	Külso auditor	Évente egyszer
	PKI alkalmazás	Külso auditor	Évente egyszer

2. táblázat

6.6. Életciklus technikai szabályok

6.6.1. Rendszerfejlesztési szabályok

Az IT életciklusra vonatkozó rendszerfejlesztési szabályokat a Szolgáltató társasági szintu informatikai biztonságpolitikája és informatikai biztonsági szabályzat tartalmazza, amelyek pontosan meghatározzák az elokészítés, a projekt, a muködtetés, a menedzselés és a visszavonás/rekonstrukció ciklus idoszakok feladatait és az alkalmazott módszertanokat.

6.6.2. Biztonságkezelési szabályok

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

6.6.3. Életciklus biztonsági értékelések

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

6.7. Hálózati biztonsági szabályok

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

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

A Szolgáltató hitelesítés-szolgáltatást, idobélyegzést és OCSP-t támogató informatikai rendszerénél a védett belso és a külso hálózatok biztonságos elválasztását tuzfal és betörés figyelo rendszer (IDS) biztosítja.

A Hitelesíto Központ közvetlen külso kommunikációt nem folytat a végfelhasználókkal.

6.8. Kriptográfiai (HSM) modul ellenorzése

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

a. a memóriájában levo magánkulcsot törli

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

7. Tanúsítvány és kulcs-visszavonási profil

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

7.1. Tanúsítvány profil

7.1.1. Alap mezok

A Szolgáltató az RFC 2459-nek megfelelo 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 megfelelo tanúsítvány kiterjesztéseket támogatja.

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

7.2. Kulcs-visszavonási profil

A Szolgáltató 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 Elofizeto és Érintett fél alkalmazása és eljárása felelos. Szolgáltató semmilyen körülmények között nem hibáztatható a kiterjesztések figyelmen kívül hagyása vagy téves értelmezése miatt.

7.3. Idobélyeg profil

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

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 Politika és Szabályozási Csoport muködik, amely a HSZSZ-M karbantartásáért felelos. A változtatási igényeket e csoport gyujti, a módosításokat elvégzi, a belso és külso tájékoztatási kötelezettségeknek eleget tesz, s a változtatásokat életbe lépteti.

A változtatásokat gyujtve a Hitelesítési Politika és Szabályozási Csoport belso nem nyilvános munkaváltozatokat hoz létre a szabályzatokból, melyek a közzététel elott belso felülvizsgálaton esnek át. A Szolgáltató a változásokat kötegelve szerkeszti új szabályzati változattá, törekedve arra, hogy új szabályzatot csak a leheto 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 jelentosebb módosítás, melyet a Szolgáltató csak az újonnan kibocsátásra kerülo tanúsítványok esetében alkalmaz (s a már kibocsátottak esetében nem) a HSZSZ-M verziószámának fo 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 belso biztonsági és egyéb szabályzattal, operatív szintu eloírással 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 megfeleloségi vizsgálatot a Szolgáltató, illetve a külso auditor is elvégzi a 2. táblázatban megadott rendszerességgel.

A szabályzat törvényeknek való megfeleloségét a Nemzeti Hírközlési Hatóság vizsgálja a HSZSZ-M aktuális változatának hatálybalépését megelozoen.

Módosítás esetén a Szolgáltató a HSZSZ-M-t, annak a változtatásokkal egybeszerkesztett új verzióját, hatósági felülvizsgálat és nyilvántartásba vétel céljából átadja a Nemzeti Hírközlési Hatóságnak. A Szolgáltató alkalmanként ezt megelozoen 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 törvényeket, kormányrendeleteket, MeH rendeleteket, ajánlásokat és szabványokat az 1.2.2 fejezet tartalmazza.

A Szolgáltató hivatkozott szabályzatai:

A MÁV INFORMATIKA Kft. Szervezeti és Muködési Szabályzata,

A MÁV INFORMATIKA Kft. Iratkezelési Szabályzata

A MÁV INFORMATIKA Kft. Titokvédelmi Szabályzata

A MÁV INFORMATIKA Kft. Informatikai Biztonságpolitikája

A MÁV INFORMATIKA Kft. Informatikai Biztonsági Szabályzata

Hitelesítési Rend Minosített Tanúsítványokhoz (HR-MTT)

Idobélyegzési Szolgáltatási Rend (ISZR)

Általános Szerzodési Feltételek a Minosített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz (ÁSZF-M)

A PKI Szolgáltatások Biztonsági Szabályzata

A PKI Szolgáltatás ok Üzletmenet-folytonossági Terve

A PK Szolgáltatások Üzemeltetési Kézikönyve

9.2. Meghatározások

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

Aláírás-ellenorzo adat: olyan egyedi adat (jellemzoen kriptográfiai nyilvános kulcs), amelyet az elektronikusan aláírt elektronikus dokumentumot megismero személy az elektronikus aláírás ellenorzésére 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 tevo aláírás-létrehozó eszköz

Biztonsági tisztviselo, biztonsági menedzser: a hitelesítés-szolgáltatás biztonságáért általánosan felelos személy

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

Elektronikus aláírás ellenorzése: az elektronikusan aláírt elektronikus dokumentum aláíráskori, illetve ellenorzéskori tartalmának összevetése, továbbá az aláíró személyének azonosítása a dokumentumon szereplo, illetve a hitelesítés-szolgáltató által közzétett aláírás-ellenorzo adat, tanúsítvány visszavonási információk, valamint a tanúsítvány felhasználásával

Elektronikus aláírás felhasználása: elektronikus adat elektronikus aláírással történo ellátása, illetve elektronikus aláírás ellenorzése

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

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

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

Elektronikus aláírási termék: olyan szoftver vagy hardver, illetve más elektronikus aláírás alkalmazáshoz kapcsolódó összetevo, amely elektronikus aláírással kapcsolatos szolgáltatások nyújtásához, így különösen elektronikus aláírások, illetoleg idobélyegzo készítéséhez vagy ellenorzéséhez használható

Elektronikus dokumentum: elektronikus eszköz útján értelmezheto adategyüttes

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

Elektronikus okirat: olyan elektronikus irat, amely nyilatkozattételt, illetoleg nyilatkozat elfogadását, vagy nyilatkozat kötelezonek elismerését foglalja magában

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

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

a. alkalmas az aláíró azonosítására,

b. egyedülállóan az aláíróhoz kötheto,

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 követoen a dokumentumon tett - módosítás érzékelheto

Hitelesítési rend: olyan szabálygyujtemény, amelyben egy szolgáltató, igénybe vevo vagy más személy (szervezet) valamely tanúsítvány felhasználásának feltételeit írja elo igénybe vevok valamely közös biztonsági követelményekkel rendelkezo csoportja, illetoleg meghatározott alkalmazások számára

Idobélyegzo: elektronikus dokumentumhoz végérvényesen hozzárendelt, vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikus dokumentum az idobélyegzés elhelyezésének idopontjában változatlan formában létezett

Idobélyegzés szolgáltatási rend: olyan szabálygyujtemény, amelyben egy szolgáltató, igénybe vevo vagy más személy (szervezet) valamely idobélyegzo felhasználásának feltételeit írja elo igénybe vevok valamely közös biztonsági követelményekkel rendelkezo csoportja, illetoleg meghatározott alkalmazások számára

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

Igénylo: a minosített tanúsítvány iránti igényt benyújtó személy

Informatikai rendszer: a szolgáltató által a szolgáltatói kulcspár kezeléséhez, az aláírás-létrehozó adat eloállításához, 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 vezérlo egyedi jelsorozat, amelynek ismerete a rejtjelezéshez vagy a visszaállításhoz, különösen az elektronikus aláírás eloállításához vagy ellenorzéséhez szükséges

Lenyomat: olyan meghatározott hosszúságú, az elektronikus dokumentumhoz rendelt bitsorozat, amelynek képzése során a használt eljárás (lenyomatképzo eljárás) a képzés idopontjában teljesíti a következo feltételeket:

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

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

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

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

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

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

Minosített tanúsítvány: az Eat. 2. számú mellékletében foglalt követelményeknek megfelelo olyan tanúsítvány, amelyet minosített szolgáltató bocsátott ki

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

Rendszerüzemelteto: az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végzo személy

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

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

Szolgáltatási szabályzat: az Eat. 6. § (1) bekezdése szerinti szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb muködési 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 idobélyegzést nyújtó szolgáltató saját elektronikus aláírási szolgáltatásának igazolására, így különösen a tanúsítvány kibocsátására, a visszavonási nyilvántartásokra, az idobélyegzésre, a naplózáshoz, az archiváláshoz használ

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

Tanúsítvány: hitelesítés-szolgáltató által kibocsátott igazolás, amely az aláírásellenorzo adatot az Eat. 9. § (3), illetoleg (4) bekezdése szerint egy meghatározott személyhez kapcsolja, és igazolja e személy személyazonosságát vagy valamely más tény fennállását, ideértve a hatósági (hivatali) jelleget

Tanúsítvány kibocsátása: a tanúsítvány átadása az aláírónak, valamint a szolgáltató nyilvántartásában a tanúsítvány elérhetové 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, illetoleg a visszavont tanúsítványokról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás idopontját